Technická univerzita v Liberci
Hospodářská fakulta

Studijní program: Systémové inženýrství a informatika (6209T)
Studijní obor: Manažerská informatika (M 6209)

Problematika systémové bezpečnosti IS/IT organizace

Problems of IS/IT system security in organization

Číslo práce: DP – MI – KIN – 2006 06

Vít Komárek

Vedoucí práce: doc. Ing. Jan Skrbek, Dr. (KIN)
Konzultant: RNDr. Milan Pilný (OR-CZ, spol. s r.o.)

Počet stran: 108 **Počet příloh: 8**
Datum odevzdání: 6.1.2006

Prohlášení

Byl jsem seznámen s tím, že na mou diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, zejména § 60 - školní dílo.

Beru na vědomí, že Technická univerzita v Liberci (TUL) nezasahuje do mých autorských práv užitím mé diplomové práce pro vnitřní potřebu TUL.

Užiji-li diplomovou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědom povinnosti informovat o této skutečnosti TUL; v tomto případě má TUL právo ode mne požadovat úhradu nákladů, které vynaložila na vytvoření díla, až do jejich skutečné výše.

Diplomovou práci jsem vypracoval samostatně s použitím uvedené literatury a na základě konzultací s vedoucím diplomové práce a konzultantem.

Datum: 28.12.2005

Podpis:

Touto cestou bych chtěl poděkovat panu docentu Skrbkovi za vedení mé diplomové práce.

Resumé

Práce se zaměřuje na představení problematiky systémové bezpečnosti IS/IT organizace. První část je věnována úvodu do problematiky, tedy definování základních pojmů souvisejících s bezpečností IS/IT. Část druhá se věnuje vybraným bezpečnostním rizikům, kde jsem se snažil o vybrání aktuálních témat. V části třetí jsou představeny některé technologické prostředky umožňující snižování těchto bezpečnostních rizik. Poslední čtvrtá část předkládá modelovou situaci řešení řízení bezpečnosti ve výrobním podniku s přibližně 100 zaměstnanci, kde se uplatní teoretické poznatky z předcházejících třech částí. Tento text navazuje na moji bakalářskou práci [08], která se mimo jiné zabývala problémy automatické identifikace osob a řešením fyzického přístupu k citlivým místům - což jsou témata s bezpečností IS přímo související.

Abstract

Study deals with the introduction to the world of IS/IT system security in organization. First part of the study addresses basic themes that are in connection with IS security. Second part focuses more deeply on chosen security risks, where I tried to choose actual and interesting topics. Third part describes some technological means which can be used in lessening these risks. And the last fourth part introduces the schematic model of integrating IS/IT system security into middle-sized manufacturing organization with approx. one hundred employees, where theoretical knowledge from previous three chapters will be applied. This text is a follow up to my previous work [08], where among others I dealt with issue of using Automated Identification of persons in labor environment and how we can solve problems with physical access to sensitive places – topics in close connection with IS/IT system security.

Klíčová slova

systémy informační
bezpečnost
data
ochrana
politika
riziko

Obsah

Seznam obrázků, schémat, tabulek

Seznam zkratek

AIT - Advanced Intelligent Tape (pokročilá inteligentní páska)
AP - Access Point (přístupový bod do bezdrátové sítě)
ATA - Advanced Technology Attachment (technologicky pokročilé připojení, rozhraní pevných disků)
BP - Bezpečnostní politika
CD - Compact Disc (kompaktní disk)
CRC - Cyclic Redundancy Check (cyklická redundantní kontrola)
ČSN - Česká státní norma
DAS - Direct Attached Storage (přímo připojené úložiště)
DAT - Digital Audio Tape (digitální audio páska)
DOS - Denial of Service (odepření služby)
DDOS - Distributed DOS (distribuovaný DOS útok)
DLT - Digital Linear Tape (digitální lineární páska)
DNS - Domain Name System (doménový pojmenovávací systém)
DVD - Digital Versatile Disc (digitální víceúčelový disk)
FDD - Floppy Disk Drive (disketová mechanika)
FTP - File Transfer Protocol (protokol pro přenos souborů)
HDD - Hard Disk Drive (pevný disk)
HTML - Hypertext Markup Language (hypertextový značkovací jazyk)
HTTP - HyperText Transfer Protocol (protokol pro přenos hypertextu)
HTTPS - HTTP + SSL
HW - Hardware
IM - Instant messaging (okamžité posílání zpráv)
IS - Informační systém
iSCSI - Internet SCSI
IT - Informační technologie
LAN - Local Area Network (místní síť)
NAS - Network Attached Storage (úložiště připojené sítí)
OS - Operační systém
PC - Personal Computer (osobní počítač)
P2P - Peer to Peer aplikace (klient x klient aplikace)
RAID - Redundant Array of Independent Disks (vícenásobně jištěné pole nezávislých disků)
RFC - Request for Comments (žádáme komentář)
S-HTTP - Secure HTTP (bezpečné HTTP)
SAN - Storage Area Network (síť pro ukládání)
SANS - SysAdmin, Audit, Network, Security Institut
SATA - Serial ATA (sériová ATA)
SCSI - Small Computer System Interface (standardní komunikační rozhraní)
SMS - Short Message Service (krátká textová zpráva)
SP2 - Service Pack 2 (opravný balík 2)
SSH - Secure Shell (bezpečný shell)
SSID - Service Set IDentifier (identifikátor bezdrátové sítě)
SSL - Secure Sockets Layer (bezpečná komunikační vrstva)
STP - Shielded Twisted Pair (stíněná dvoulinka)
SW - Software
URL - Uniform Resource Locator (internetový ekvivalent pro adresu)
USB - Universal Serial Bus (universální sériová sběrnice)
UTP - Unshielded Twisted Pair (nestíněná kroucená dvoulinka)
WAN - Wide Area Network (rozlehlá síť)
WEP - Wireless Encryption Protocol (bezdrátový šifrovací protokol)
WPA - Wireless Protected Access (chráněný bezdrátový přístup)

1. Úvod

Nasazení informačních systémů a informačních technologií se v dnešní době stalo nutnou podmínkou úspěšnosti (ne-li dokonce přežití) firem ve všech oblastech hospodářské činnosti. IS/IT jsou již několik let jedním z rozhodujících faktorů rozvoje a konkurenceschopnosti hospodářských organizací ve všech třech sektorech. Bez informačních technologií je v dnešní době práce s informacemi nejen neefektivní, ale již i nemožná. Navíc s každým dnem naše závislost na těchto systémech roste. S rychlým rozvojem moderních technologií informačních systémů však roste i možnost jejich zneužití.

Na denním pořádku jsou nejrůznější bezpečnostní incidenty, například neoprávněná manipulace dat (ať už se jedná o smazání, změnu, odcizení a následné zneužití), zastavení chodu celé organizace díky kolapsu napadeného informačního systému a další.

Za první polovinu roku 2005 společnost IBM zaznamenala 237 miliónů bezpečnostních útoků, což představuje 50 procentní zvýšení oproti období minulému. Skutečné číslo však bude jistě mnohem vyšší. Hlavními cíli přitom byla státní správa, výrobní odvětví, finanční odvětví a zdravotnictví. [I-12]. Přičemž podle počtu „úspěšných“ průniků můžeme říct, že jen velmi málo podniků má zavedenou fungující bezpečnostní strategii. [I-05]

Podle organizace Computer Economics (http://www.computereconomics.com/) škody z těchto útoků šplhají do biliónů; jen samotná epidemie viru MyDoom způsobila celosvětově odhadem škodu za 4 miliardy dolarů. Podle studie společnosti McAfee Security stojí firmu každý úspěšný virový útok v průměru 5000 eur (omezení / přerušení provozu a následné odstraňování škod). Údaje z těchto a jim podobných studií nemusí sice být zcela přesné, ale rozhodně je nelze nebrat v úvahu.

A nejde jen o cílené útoky. Dnešním Internetem navíc neustále kolují další necílené hrozby hledající jakoukoli možnou skulinu v zabezpečení stanic. Podle Internet Storm Centra [I-02] (člena SANS institutu) je nezáplatované PC s operačním systémem Windows po zapojení do Internetu napadeno v průměru do dvaceti minut, což představuje dvojnásobný nárůst oproti roku 2003, kdy tato doba zabrala cca. minut čtyřicet. Toto snížení tzv. “survival time” je považováno za velice vážný skok – tato doba je totiž kratší než doba potřebná pro zaktualizování zabezpečení počítače přes vydané záplaty proti neoprávněným přístupům a útokům.

Pak tedy i běžný uživatel s nezabezpečeným počítačem je v ohrožení, neb i bez jeho vlastního přičinění (prohlížení stránek s pochybným obsahem, spouštění nelegálních kopií programů, užívání P2P sítí atd.) může mnoha způsoby (email, přílohy emailu, pouhé zapojení PC do sítě, CD, mobil atd.) nevědomky poskytnout přístup do svého celého počítače k soukromým údajům, o které pak může během chvíle i přijít.

Ukazuje se, že donedávna poměrně opomíjené téma zabezpečení informačních systémů již nadále opomíjet nelze. Uvědomuje si to již takřka každý, kdo má se světem IS/IT něco společného.

Díky počáteční neznalosti této problematiky mezi jak veřejností, tak i velkou částí IS/IT obce administrátorské, programátorské a uživatelské se pojem bezpečnost stal i dobrým obchodním artiklem (a to teď vůbec nekomentuji zvýšené zisky společností zabývajících se vývojem / výrobou prostředků pro zabezpečení IS/IT, poradenských firem a všemi dalšími, kteří dokázali danou situaci využít ve svůj prospěch - zisky těchto firem stoupají meziročně o desítky procent [I-03]).

IS/IT informační portály, žijící z počtu zobrazení reklam na svých stránkách, mající kdysi prázdné sekce s názvy jako bezpečnost, viry, spyware teď obsahují každý týden nové články o aktuálním dění. Dokonce s touto tématikou vznikají i nové samostatné portály. Články na téma bezpečnosti se dostaly i do periodik, která s IS/IT ani přímo nesouvisí (za všechny jmenujme alespoň Instinkt, Security magazín atd.).

Vydavatelé knih ve světě v uplynulých letech začali doslova zahrnovat trh čímkoli, co v názvu obsahuje v jakémkoli kontextu slovo bezpečnost. Čeští vydavatelé nezůstávají pozadu a toto překládají, přičemž jim nevadí, že většina těch knih měla nějaký význam v době svého vydání a dnes jsou z větší části tyto knihy již neaktuální a překonané, obsahují postupy v naší firemní realitě neaplikovatelné, či jsou velice specificky zaměřené. Velice snadno se dá ztratit přehled, protože dobrých a aktuálních knih umožňujících prvotní seznámení s touto problematikou nenajdeme u nás mnoho. ([01], [06], ze starších [03] a [02]).

Cílem této práce je proto poskytnout základní a globální pohled na aktuální problematiku informační bezpečnosti, rozvinout vybrané problémy a naznačit možná řešení / postupy vedoucí ke snížení bezpečnostních rizik.

Práce je rozdělena na čtyři části: První část je věnována úvodu do problematiky, tedy definování základních pojmů souvisejících s bezpečností IS/IT. Druhá část popisuje vybraná současná bezpečnostní rizika, s kterými se potýkají dnešní IS/IT a jejich uživatelé. Třetí část informuje o způsobech, kterými lze tato rizika snižovat. Poslední čtvrtá část předkládá modelovou situaci zabezpečení sítě menšího výrobního podniku s přibližně 100 zaměstnanci, kde se uplatní teoretické poznatky z předcházejících třech částí.

Na některých místech v textu budu odkazovat na svoji předcházející práci vypracovanou za účelem získaní bakalářského titulu s názvem: **Problematika identifikace osob v běžném provozu organizace [8],** která mimo jiné řešila problémy automatické identifikace osob a řešení fyzického přístupu k citlivým místům - což jsou témata přímo související s bezpečností IS/IT.

2. Úvod do problematiky systémové bezpečnosti IS/IT

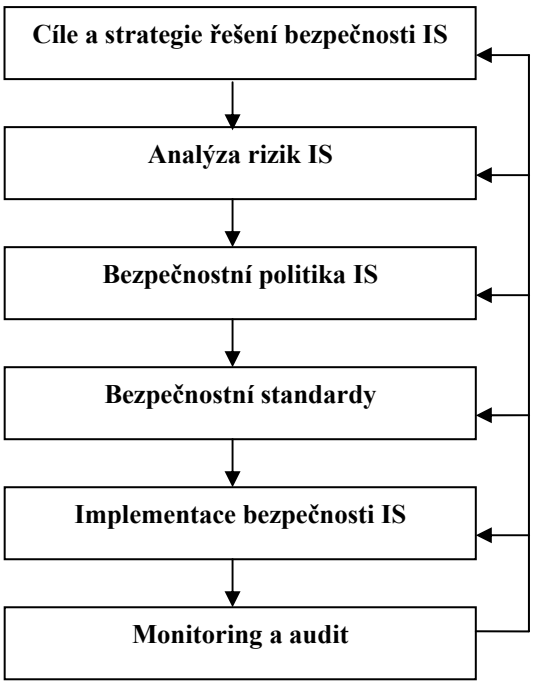
Definice: Bezpečnost IS/IT

"Proces dosažení a udržení důvěrnosti, integrity, dostupnosti, účtovatelnosti, autenticity, spolehlivosti informací a IT služeb na přiměřené úrovni." [07]

"Ochrana informací během jejich vzniku, zpracování, ukládání, přenosů a likvidace prostřednictvím logických, technických, fyzických a organizačních opatření, která musí působit proti ztrátě důvěrnosti, integrity a dostupnosti těchto hodnot." [02]

V této kapitole budu volně postupovat podle následujícího schématu. (schéma vychází z mezinárodního bezpečnostního standardu ISO 13335). Vzhledem k omezenému rozsahu práce bude stupeň rozpracování jednotlivých částí procesu řízení bezpečnosti záviset na jejich vazbě k dalším kapitolám.

Schéma číslo 1: Proces řízení bezpečnosti podle ISO 13335



Zdroj: [07]

2.1 Bezpečnostní politiky a systémová bezpečnost IS/IT

Řízení bezpečnosti je v organizaci formulováno na základě následujících tří bezpečnostních politik:

Celková bezpečnostní politika organizace představuje souhrn bezpečnostních zásad a předpisů, které definují způsob zabezpečení organizace jako celku (od fyzické ostrahy, přes ochranu soukromí až po ochranu lidských práv).

Celková bezpečnostní politika IT organizace je manažerským pohledem na bezpečnost IT, kráčí ve stopách celkové bezpečnostní politiky, definuje základní strategii, cíle, postoje, role, zodpovědnosti a zásady týkající se činností spojených s bezpečností IT organizace (určuje rámec bezpečnosti). Celková bezpečnostní politika je základním informačním zdrojem při budování nižších a specifických stupňů bezpečnostní dokumentace.

Bezpečnostní politika IS (systémová bezpečnostní politika IT/IS) již konkrétně definuje, jakým způsobem bude přijata a realizována celková bezpečností politika IT pro konkrétní IS. Obsahuje detailní normy, pravidla, praktiky a předpisy konkrétně definující způsob správy, ochrany a distribuce citlivé informace a jiných IT zdrojů v rámci organizace a konkrétního IS. Principy zpracování bezpečnostní politiky IS jsou formulovány na základě stanovených požadavků v oblasti počítačové bezpečnosti, systémových bezpečnostních požadavků daného IS, dokumentu celkové bezpečnostní politiky IT, výsledků analýzy rizik IS, bezpečnostních požadavků uvedených v zákonech, vyhláškách, normách, předpisech a standardech.

V literatuře pojmy celková bezpečnostní politika IT a bezpečnostní politika IS často splývají pod jednotný název bezpečnostní politika (zkratka BP), respektive systémová bezpečnostní politika.

2.2 Cíle bezpečnosti v IS a bezpečný informační systém

Typická, pro většinu společností vyhovující definice cíle může znít: „Základním cílem je eliminovat případné přímé a nepřímé ztráty způsobené zneužitím, poškozením, zničením, nebo nedostupností informací, vytvořením uceleného, nákladově optimalizovaného a efektivně fungujícího systému řízení bezpečnosti informací.“ [12]

Tři základní pravidla, která definují cíle bezpečnosti v IS:

- **zajištění důvěrnosti a integrity utajované informace** všude, kde se vyskytuje,
- **zajištění dostupnosti informace a služeb informačního systému**
- **zajištění odpovědnosti uživatele informačního systému** za jeho činnost v něm.

Abychom dodrželi tato na první pohled jednoduchá pravidla a mohli o našem systému říct, že se jedná o systém bezpečný, musí splňovat několik požadavků. Systém musí být schopen nějakým způsobem **rozpoznat uživatele**. Procesu rozpoznávání uživatele se také jinak říká ověřování totožnosti / autentizace. Osoba přistupující do IS musí prokázat, že je opravdu tou osobou, pod kterou hodlá do systému přistupovat a využívat jeho služeb. Tomuto prokázání totožnosti se říká "důkaz" a v současnosti se používají čtyři typy důkazů (či jejich kombinace) a to: důkaz znalostí, vlastnictvím, vlastností, činností (více viz. [08]). Systém pak již rozhodne, zda danou osobu do systému pustí, či "spustí alarm".

Po vpuštění uživatele do systému musí tento systém disponovat mechanismy pro **usměrnění** (řízení) jeho **přístupu** - kromě domácích PC snad neexistuje situace, kdy by uživatelé jednoho počítače / systému měli všichni totožná práva. Pomocí autorizace (oprávněnost) máme možnost přidělovat práva na informace a akce (povolit, schválit, zmocnit, oprávnit). Nejčastěji se používá systém tzv. rolí - vytvoří se role (soubor přístupových práv) pro všechny existující typy uživatelů / administrátorů IS, tyto role se potom přiřazují jednotlivým uživatelům / administrátorům. Po přihlášení do systému se tedy načte uživatelova role a dojde ke zpřístupnění náležitých částí systému. Dbát se musí samozřejmě na to, aby kromě oprávněných osob nikdo jiný nemohl přístupové role měnit, ať už sobě nebo jiným.

Bezpečný IS dále musí zajistit **důvěrnost informací.** Tím se zjednodušeně myslí, že nikdo neoprávněný nesmí mít šanci tato data vidět. K zajištění tohoto se používá již zmiňovaná kontrola přístupu a dále šifrování. Samozřejmostí je **nedotknutelnost informací** (zajistit integritu dat); nikdo nepovolaný nesmí data měnit. V praxi se používají např. jednosměrné funkce (algoritmy HASH) a digitální podpisy. **Informace** poskytované bezpečným IS musí být **dostupné** vždy, **kdy** jsou **potřeba.** A jako poslední, tento systém by měl **zaznamenávat** všechny probíhající **činnosti**, aby se zpětně dalo při auditu zjistit, zda-li nedošlo k nějakému bezpečnostnímu incidentu a v případě jeho výskytu odhalit co, nebo kdo bylo / byl jeho příčinou.

Protože se každý IS skládá z několika částí, může být bezpečný IS vybudován pouze použitím komplexních ochranných mechanismů.

2.3 Proč vůbec zabezpečovat IS/IT

Má-li mít snaha o zabezpečení systému šanci na úspěch, je bezpodmínečně nutné o nezbytnosti a prospěšnosti tohoto kroku přesvědčit vedení společnosti.

Zabezpečení IS/IT neznamená jenom nakoupit nějaký HW a SW (kromě nejzákladnějších a ne moc účinných forem zabezpečení), tento proces vyžaduje vypracování souboru interních směrnic a předpisů, které musí být respektovány a bezvýhradně dodržovány. Přičemž jako vždy

v odvětví IS/IT, největším problémem při zavádění změn se ukazuje postoj běžných uživatelů, jejichž myšlení se musí změnit. A této změny v organizaci nelze dosáhnout z pozice bezpečnostního pracovníka / pracovníků existujících někde v zapadlém koutu výpočetního střediska, hluboko v organizační struktuře.

Podpora managementu je proto klíčovým předpokladem úspěchu projektu. Právě díky nezískání této podpory mnoho bezpečnostních projektů bez ohledu na jejich kvalitu skončí prvotním návrhem na papíře, nebo v různem stupni rozpracování s jediným efektem, a to zbytečně vynaloženými prostředky a silami administrátorů / bezpečnostních pracovníků IS. Je tedy jistě dobré připravit si k přesvědčení vhodné argumenty.

Nasazení bezpečnostních opatření (bezpečnostní politiky, viz další část této kapitoly) sice **negeneruje žádný** okamžitý **přímý zisk do organizace** - naopak investice na její zavedení a údržbu nejsou nijak zanedbatelné. **V případě mimořádných událostí se však stává nedocenitelnou.** Hlavní význam bezpečnostní politiky je prevence. V dlouhodobém období je v dnešní době nezbytnou součástí celkové bezpečnostní politiky organizace.

Bezpečnostní politika chrání firemní investice (hardware & software & know-how). Certifikáty o zabezpečení IS/IT zvyšují firemní důvěryhodnost - konkurenční výhoda s v dnešní době nezanedbatelným významem. Zároveň bezpečnostní politika předchází poškození dobrého jména společnosti "medializací" úniku dat tím, že možnost jejich úniku takřka eliminuje. A pro případ, že by k nějakému úniku přeci jen došlo, BP má přesné směrnice (nazývají se havarijní plán), jak se zachovat, a je argumentem proti nařčení o nedůvěryhodnosti. Podrobné sledování celého systému zablokuje nelegální aktivity dříve, než dojde ke škodě, anebo alespoň ihned odhalí slabá místa a tím znemožní opakovaný únik informací stejnou cestou.

BP ale hlavně v dnešní době řeší problémy mnohem „hmatatelnějšího" rázu. Poskytuje ochranu před hackery a dalšími potencionálními útočníky, kteří se snaží proniknout do IS za účelem průmyslové špionáže / vlastního obohacení / jen tak pro zábavu / ze zášti atd.. Zvyšuje odolnost IS společnosti před napadením počítačovými viry (v roce 2004 jedna z největších hrozeb organizacím vůbec), stejně tak blokuje ostatní škodlivé programy jako trojské koně (umožňující vytvoření zadních vrátek do firemního systému a následnému vyzrazení / zcizení důvěrných údajů - databáze smluv, klientů apod.), odfiltruje většinu spyware a jemu podobné škodlivé programy.

BP také má připravený plán pro případ nenadálých událostí, ať už se jedná o selhání technického zařízení, nebo přírodní pohromu.

"**Investice do prevence bezpečnosti IS je ve výsledku mnohem levnější než řešení následných škod**. " [07]

2.4 Analýza rizik IS

Cílem jakékoli analýzy rizik v rámci organizace je identifikovat a kvantifikovat rizika tak, aby bylo možné rozhodnout o jejich přijatelnosti, anebo rozhodnout o přijmutí dodatečných opatření k jejich snížení. Velikost rizika je stanovena na základě pravděpodobnosti výskytu rizika a velikosti dopadu.

Analýza rizik IS je klíčovou aktivitou v procesu řešení bezpečnosti, která musí poskytnout odpověď na následující tři základní otázky: „Co se stane, když nebudou informace chráněny?“, „Jak může být porušena bezpečnost informací?“, „S jakou pravděpodobností se to stane?“. Typickým výstupem analýzy je dokument obsahující popis systému a výsledky analýzy, tedy úroveň hrozeb, zjištěné zranitelnosti, úroveň stávajících ochranných opatření a distribuci výsledných rizik. Vzhledem k významu řízení rizik pro dnešní IS byla analýza rizik v IS podrobněji popsána a její provádění je vyžadováno v některých standardech v oblasti řízení bezpečnosti, např. BS7799 a v ISO/IEC TR 13335. **ISO/IEC TR 13335 definuje bezpečnost jako zachování důvěrnosti, integrity, dostupnosti, individuální zodpovědnosti, autenticity a spolehlivosti.** Cílem řízení rizik je tedy zachování těchto kvalit informací.

Protože provedení podrobné analýzy rizik pro rozsáhlé IS by bylo časově velice náročné a informační rizika hrozící určitým typům organizací nejsou zase až tak vysoká, aby bylo třeba tuto analýzu provádět opravdu důkladně, definuje standard ISO/IEC TR 13335 čtyři různé stupně přístupu k provádění analýzy rizik**: základní, neformální, podrobný a kombinovaný.**

2.4.1. Základní přístup

Jedná se o metodu rychlého zavedení určitých bezpečnostních opatření bez podrobnější analýzy. Tato sada opatření je obvykle přejata z některého standardu v oblasti informační bezpečnosti nebo z katalogů ochranných opatření (součást dokumentace některých softwarových nástrojů). Ze sady se potom vyberou ta pravidla, které mají relevantní význam pro danou organizaci, dojde k porovnání stávajících bezpečnostních opatření proti těm nově vybraným a ta pravidla, co dosud nejsou zavedena a měla by být, jsou implementována.

Největší výhodou této metody je pochopitelně její rychlost. Analýza rizik spotřebuje minimální množství zdrojů. Také lze ušetřit při samotné implementaci – při aplikaci standardních bezpečnostních opatření lze v mnoha případech použít standardních řešení (platí hlavně pro rámec jedné společnosti, stejná opatření pro všechny divize, dceřiné společnosti atd.).

Ovšem na druhou stranu, z nasazení předem definovaných sad opatření bez ohledu na analýzu rizik odhalující skutečnou potřebu úrovňe bezpečnosti v jednotlivých oblastech plyne řada nevýhod. V některých částech bude ochrana nedostatečná, v jiných zase zbytečně vysoká

(zbytečně vynaložené prostředky). Další problémy nastanou při změnách v systému - bude obtížné určit dopad změn na úroveň bezpečnosti a rozhodnout o dodatečných bezpečnostních opatřeních.

Tento systém je nejvhodnější pro organizace s menší závislostí na IT, která nemá vysoké nároky na úroveň bezpečnostních požadavků. Zároveň musí mít všechny části organizace podobnou potřebu ochrany - tam, kde jsou požadavky na ochranu v jednotlivých částech výrazně odlišné, je třeba použít jiného přístupu.

2.4.2. Neformální přístup

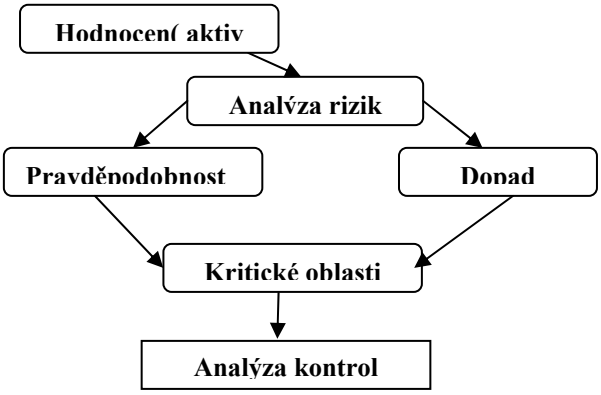
Přístup založený nikoli na definovaných metodologiích, ale vycházející ze zkušenosti jednotlivců a jejich znalosti prostředí. Výhodou je rychlost a nenákladnost. Nevýhodou je právě závislost kvality opatření na znalostech a zkušenostech daných jednotlivců. A díky rychlosti pokroku dnešního světa IS/IT je těch novinek tolik, že je takřka nemožné pro kohokoli udržet si dostatečný přehled o všech oblastech a při provádění analýzy nějakou část neopomenout. Další nevýhodou je špatná obhajitelnost výsledku analýzy založené na zkušenostech a ne na nějaké definované metodologii. Tento problém se ještě prohloubí, když osoba provádějící tuto analýzu organizaci opustí.

Tato metoda se dá doporučit pouze jako první krok v případech, kdy je nutné takřka okamžitě zvýšit úroveň bezpečnosti.

2.4.3 Podrobná analýza rizik

Nejpřesnější, zároveň ale časově i finančně nejnáročnější metoda analýzy rizik. Při této analýze se postupuje podle následujících kroků: identifikace a ohodnocení aktiv > posouzení hrozeb pro tato aktiva > odhad zranitelností. Výsledky této analýzy jsou poté použity k odhadu rizik a na základě tohoto odhadu jsou vybrána odpovídající bezpečnostní opatření.

Schéma číslo 2: Podrobná analýza rizik



Zdroj: [02]

Identifikace a hodnocení aktiv

Prvním krokem je vymezení části IS, která bude této analýze podrobena. Pro tuto část je nutno dále identifikovat všechna informační aktiva [data, SW, HW (servery, stanice, síťové prvky, komunikační vybavení apod.) a služby].

Dalším krokem je ohodnocení těchto aktiv:

- fyzická aktiva (+ SW): hodnota dána cenou náhradní komponenty a případnou ztrátou vzniklou dobou nutnou k nahrazení této komponenty,

- datová aktiva: mnohem obtížnější posouzení hodnoty, založeno na ztrátě, kterou společnost utrpí v případě zničení, poškození, nedostupnosti, nebo ztrátě důvěrnosti těchto aktiv. (hodnota těchto aktiv je odvozována nepřímo přes soustavu nepeněžních měřítek; Standard ISO/IEC TR 13335 předkládá jako doporučení vzít v úvahu alespoň následující nepeněžní parametry: nedodržení legislativy a / nebo předpisů, zhoršení výkonu činnosti organizace, ztráta dobrého jména nebo negativní vliv na pověst firmy, narušení důvěrnosti spojené s osobními informacemi, ohrožení osobní bezpečnosti, nepříznivý vliv na prosazení práva, porušení obchodního tajemství, narušení veřejného pořádku, finanční ztráty, přerušení aktivit činnosti organizace, zhoršení bezpečnosti prostředí.

Tyto nepeněžní parametry ohodnocujeme přes pomocné stupnice, kdy pro každý stupeň budeme mít jeho slovní vysvětlení. Pro každý parametr a jeho hodnoty (stupnice 1-10) je také vhodné určit přibližné následky pro společnost ve finančních jednotkách tak, abychom mohli alespoň přibližně (rozumný odhad) získat jednotné měřítko hodnoty aktiv. Je jasné, že pomocí tohoto postupu nikdy nedosáhneme přesného odhadu hodnoty aktiva (zvlášť, pokud se jedná o aktiva typu "data" nebo „služba"), ale o to ani v praxi nejde. Důležité je získat alespoň přibližné roztřídění aktiv IS do několika skupin (např. kritická, významná, ostatní a další …). Toto roztřídění do skupin je už poměrně spolehlivé, pro účely analýzy rizik dostatečné a není třeba dlouze diskutovat o přesných finančních hodnotách nebo přesném pořadí aktiv z hlediska hodnoty.

Nejsložitější úlohou při ohodnocení aktiv je určení vzájemné závislosti mezi aktivy (např. „pokud nebude fungovat toto, pak bude nedostupné to a to") a promítnutí těchto vztahů do hodnoty aktiv. Pro tento proces nelze dát jednoznačný návod, ale obecně platí, že pokud hodnota závislého aktiva je větší než hodnota aktiva právě posuzovaného, je třeba zvážit zvýšení jeho hodnoty.

Konečným výstupem tohoto kroku je seznam aktiv a jejich hodnot s ohledem na jejich zpřístupnění neautorizovaným osobám (ochrana důvěrnosti), modifikaci (ochrana integrity), nedostupnosti a zničení (ochrana dostupnosti) a náklady na nahrazení aktiv. Součástí tohoto výstupu bývá také schéma systému, které ukazuje vzájemné vazby jednotlivých aktiv.

Posouzení hrozeb

Základní charakteristika hrozeb je obsažena v přílohách (příloha č.1: Pojmy spojené s analýzou rizik: Hrozba, Zranitelné místo, Útočníci). V procesu posuzování hrozeb je prvním krokem identifikace jednotlivých kategorií hrozeb. K tomu existují již předem připravené katalogy se seznamem všech možných hrozeb (např. v příloze normu ISO/IEC TR 13335, nutno neustále doplňovat o nově se objevující hrozby). V druhém kroku je třeba provést odhad pravděpodobnosti výskytu hrozby. Informace o pravděpodobnosti jsou získány podle typu hrozby buď z interních (uživatelé a správci systému) nebo externích zdrojů (statistiky požárů nebo přírodních katastrof pro danou lokalitu).

Výstupem tohoto kroku je seznam hrozeb, které připadají pro daný IS v úvahu, seznam aktiv nebo skupiny aktiv, které mohou být těmito hrozbami ovlivněny, a míra pravděpodobnosti výskytu hrozeb, např. na stupnici „vysoká, střední, nízká“.

Odhad zranitelnosti

Základní charakteristika zranitelných míst je obsažena v přílohách (příloha č.1: Pojmy spojené s analýzou rizik: Hrozba, Zranitelné místo, Útočníci). Analýza zranitelných míst spočívá v prozkoumání slabých míst, která mohou být využita identifikovanými hrozbami. Tyto scénáře, které popisují, jak může konkrétní hrozba nebo skupina hrozeb využít konkrétního zranitelného místa / míst se nazývají rizikové scénáře (hrozba odposlechu může využít zranitelné místo „nechráněné komunikační linky“, zranitelné místo „nedostatek dokumentace“ může být problém v případě hrozby „chyba provozních zaměstnanců“ apod.).

Výsledkem tohoto kroku je seznam zranitelností a odhad snadnosti jejich využití, např. opět s použitím stupnice „vysoká, střední, nízká“.

Výběr ochranných opatření

Ze všech zjištěných potřebných ochranných opatření jich již velké množství může být zavedeno / může být ve fázi zavádění / nebo je jejich implementace plánována. Z tohoto hlediska je tedy třeba doporučená kontrolní opatření roztřídit tak, aby bylo zřejmé, kde jsou nejvýznamnější nedostatky. Před samotným roztříděním musíme nejprve zjistit aktuální stav - obvykle přes další kola rozhovorů s uživateli, IT specialisty i vedením společnosti.

Ochranná opatření lze třídit podle různých hledisek, ale nejvýznamnější je pravděpodobně rozdělení na opatření preventivní a následná (předcházení a řešení / obnova po incidentu). Při výběru ochranných opatření je třeba dbát na to, aby pro každé riziko, které jsme se rozhodli snížit, bylo připravené jak preventivní, tak následné opatření. Zároveň je třeba vzít v úvahu vzájemnou závislost ochranných opatření mezi sebou.

Výsledkem tohoto kroku je seznam všech existujících a plánovaných ochranných opatření a stav jejich implementace a použití.

Přijetí rizik

Cílem řízení rizik není rizika eliminovat (to ani úplně není možné), ale popsat a snížit na únosnou úroveň. Po implementaci ochranných opatření zbude tzv. zbytkové riziko (kombinace faktorů jako hodnota aktiva, hrozeb, zranitelných míst a již zavedených ochranných opatření - tyto faktory jde kombinovat tak, abychom dostali kvalitativní odhad výše zbytkového rizika, jako např. vysoké, střední, nízké). Zjištěná zbytková rizika je třeba pro jednotlivé systémy identifikovat a posoudit, zda opravdu jsou pro organizaci přijatelná. Toto rozhodnutí o přijatelnosti rizik by mělo být schváleno vedením organizace. Pokud je zbytkové riziko označeno za nepřijatelné, měly by být zároveň vyčleněny prostředky na jeho pokrytí.

K zjištění zbytkového rizika lze dospět řadou způsobů [např. tabulka hrozba X zranitelnost a jednotlivé stupně k určení pravděpodobnosti uplatnění hrozby a následné porovnání jednotlivých rizik (přijatelné, poškozující, nepřijatelné) s již přijatými ochrannými opatřeními].

Ať už se ke zjištění zbytkového rizika použije jakýkoli postup, výše tohoto rizika dává zřetelné priority pro implementaci případných nových ochranných opatření.

Poznámka na závěr:

Pro analýzu rizik existují specializované programy, nástroje a postupy, např. Cobra, CRAMM, NetRecon, RiskWatch, RiskPAC aj.. Poradenské firmy také mají často vyvinuty svoje vlastní nástroje. Nejkvalitnější jsou ty nástroje, které uživatele provedou celým procesem přes série otázek, poskytnou mu databáze hrozeb, zranitelných míst a kontrolních mechanismů, dále budou obsahovat vzorové dotazníky pro další sběry informací. Zároveň by tyto nástroje měly na základě výše zbytkového rizika v jednotlivých oblastech určit, které kontroly jsou nezbytné a které naopak není třeba zavádět. Jedině tak lze plně realizovat výhody podrobné analýzy rizik a zavádět pouze ta bezpečnostní opatření, která jsou účelná.

Další kriteria pro výběr vhodného nástroje jsou například: aplikovatelnost v daném prostředí pro konkrétní účely, typ metodologie, podporované bezpečnostní standardy a normy, rozsah báze dat a možnost její editace, vyspělost a flexibilita výstupu, cena, uživatelská podpora ...

2.4.4 Kombinovaný přístup

V praxi nelze čekat několik měsíců na výsledky podrobné analýzy rizik - příliš velké riziko. Proto se používá mixu základního přístupu a podrobné analýzy. Vybraná kritická aktiva se analyzují pomocí podrobného přístupu, na ostatní části systému se použije přístup základní. Touto metodou organizace rychle získá přehled rizik hrozících jejímu IS, přičemž kritické procesy má zajištěny kvalitní podrobnou analýzou. Navíc v průběhu času lze do podrobné analýzy začlenit i méně kritické části IS a tím jeho ochranu ještě zkvalitnět.

2.4.5 Závěrečné shrnutí

Analýza rizik je základním prvkem budování systémů řízení rizik IS. Teprve na základě dobře provedené analýzy rizik lze určit, jaké kontrolní mechanismy jsou potřeba, které jsou nezbytné a které naopak nadbytečné.

Je třeba také poznamenat, že analýza rizik poskytuje informace o stavu řízení informačních rizik k jistému časovému okamžiku. Vzhledem k neustálému vývoji jak IS, tak i prostředí, ve kterém IS existuje, je třeba tuto analýzu aktualizovat. Aktualizace částí analýzy se provádějí při významných změnách IS (nová část, nová aplikace atd.) nebo při zjištění nové hrozby. Celková analýza by měla být aktualizována podle velikosti organizace a její závislosti na IT každých 12 až 36 měsíců. [07]

Možné problémy a chyby spojené s analýzou rizik

Na úplný závěr bych rád zmínil nejčastější problémy a chyby spojené s analýzou rizik tak, jak je uvádí literatura. V mnoha organizacích analýza rizik není vůbec prováděna, dojde pouze k plošnému zavedení ochranných opatření podle nějakého standardu. Plošné zavedení bezpečnostních opatření přitom vede k zbytečně velkým nákladům na bezpečnost a nezaručí dostatečnou ochranu informačního systému společnosti. Existuje také mnoho případů, kdy analýza rizik sice byla provedena, ale její výsledky nebyly využity - důsledky pak jsou stejné jako v případě plošného zavádění bez analýzy. Občas se také stane, že provedená podrobná analýza nebyla kompletní, nebo že byla zahájena, ale nebyla dokončena. V takovém případě je nutné co nejdříve dokončit alespoň analýzu základní (či neformální), jinak hrozí, že dojde k opomenutí některých významných rizik. Chybou je i pouze jednorázové provedení analýzy bez následných aktualizací - neobnovovaná analýza nezahrnuje nové komponenty IS / nová rizika pro IS a bezpečnostní opatření nebudou dostatečná. Navíc v případě potřeby aktualizace po delší době bude pravděpodobně nutné začít znovu kompletně od začátku - zbytečně vynaložené

prostředky. Problémy také může způsobit správce sítě, který se rozhodne ignorovat analýzu a místo toho se spíše spolehne na své znalosti a preference, bez objektivního vztahu k této analýze - společnost sice může vynakládat značné finanční prostředky na zabezpečení a přesto nejsou zjištěná rizika přiměřeně pokrývána a řada klíčových protiopatření nebude implementována. [05]

2.5 Bezpečnostní politika

Synonyma pro BP:

Informační bezpečnostní politika, Systémová bezpečnostní politika, Bezpečnostní politika ochrany informací.

Bezpečnostní politika je nedělitelným prvkem informačních systémů a zahrnuje **technická, fyzická, administrativní, personální, etická, ekologická, právní a sankční opatření v rámci přístupu a použití dat v informačních systémech** („politika“ v tomto případě znamená „péče o záležitosti určitého oboru.“). Má podobu dokumentu (kodexu), který je v dané společnosti (provozovateli daného IS) součástí interní legislativy a který je pro společnost závazný. Musí to být veřejně přístupný dokument. Představuje soubor norem, pravidel a praktik definující způsob správy, ochrany a distribuce citlivých dat a jiných aktiv v rámci činnosti IS, který je třeba dodržovat, aby byla zajištěna důvěrnost, ale také odpovídající dostupnost dat. Jinými slovy cílem bezpečnostní politiky je ochrana majetku, pověsti a činnosti organizace [04, srpen 2004].

BP by měla umět odpovědět na následující otázky: [01]

a) Co chceme chránit? b) Proč to chceme chránit? c) Jak to chceme chránit?

d) Jak ověříme, že je to opravdu chráněno? e) Co budeme dělat, když se něco pokazí?

Hlavní požadavek na BP je, aby byla úplná, „komplexní“ - definuje východiska pro všechny další aktivity společnosti v oblasti informační bezpečnosti - musí tedy pokrývat všechny významné rizikové oblasti **(fyzická, personální, režimová, technická, programová, datová, komunikační bezpečnost)**.

Z požadavku na úplnost ovšem ještě automaticky nevyplývá úroveň detailu a faktický rozsah politiky. Existují politiky o rozsahu 3 stran formátu A4 na straně jedné, na straně druhé některé BP mají hodně přes stovku stran. Ne / výhody krátkých a dlouhých BP jsou podrobněji rozepsány v přílohách (příloha č. 7: Srovnání výhod a nevýhod krátkých a dlouhých BP).

V případě stručných dokumentů BP obsahuje většinou pouze definice základních principů a stanovení základních odpovědností a pravomocí. Rozsáhlejší BP již podrobně řeší všechny oblasti bezpečnosti. Oba způsoby mají své výhody a nevýhody a je již jen na společnosti (vlastnících, managementu, předchozích zkušenostech, formách interní legislativy, průbězích schvalovacích procesů, apod.), jakou formu si vybere.

Východiskem pro řešení BP společnosti také mohou být uznávané světové standardy a metodiky (ITSEC, ITEM, TC SEC, ISO/IEC TR 13335, ISO/IEC 17799:2000 atd.). Při tvorbě bezpečností politiky si také musíme dát pozor na to, aby její struktura a obsah vyhovoval případným regulatorním požadavkům (například BP upravující oblast utajovaných skutečností ve smyslu zákona č. 148/1998 Sb. musí být vypracována podle vyhlášek Národního bezpečnostního úřadu apod.).

Na tomto místě bych rád stručně načrtnul základní body obecné bezpečnostní politiky. Podrobnější ukázkovou strukturu a obsah BP podle [07] uvádím do přílohy.

Tabulka číslo 1: Základní body Bezpečnostní politiky

Bod č. 1	**Úvodní část** - slovo managementu o významu BP pro firmu.
Bod č. 2	**Cíle a rozsah bezpečnostní politiky** - definice hlavních a dílčích cílů BP.
Bod č. 3	**Charakteristika IS firmy** - komponenty IS, selekce informací.
Bod č. 4	**Východiska bezpečnosti** - co má vliv na požadovanou úroveň informační bezpečnosti
Bod č. 5	**Pravidla a zásady bezpečnosti IS firmy** - výčet všech hlavních bezpečnostních pravidel a zásad, jimiž se řídí bezpečnost IS firmy.
Bod č. 6	**Řízení bezpečnosti IS firmy** - struktura bezpečnostního managementu, způsob zvládání bezpečnostních incidentů, havarijní plány, postup testování bezpečnosti atd.
Bod č. 7	**Závěrečná ustanovení** - výjimky a sankce, správa dokumentu.
Bod č. 8	**Přílohy** - kopie certifikátů, formuláře pro připomínky atd.
Bod č. 9	**Slovníček pojmů** - odborné termíny spojené s BP.

Zdroj: [07]

2.5.1 Přijetí bezpečnostní politiky:

Vytvořením bezpečnostní politiky práce samozřejmě nekončí. BP je třeba přijmout managementem a vyhlásit. V ideálním případě by byly schváleny všechna taková opatření, jejichž náklady na zavedení nepřevýší odhadnutou cenu chráněných aktiv. Skutečnost je ale velice odlišná.

Ohledně přijímání bezpečnostních opatření se literatura psaná na základě praktických zkušeností shoduje v tom, že tato fáze je jedna z nejtěžších vůbec, připomínající někdy „boj s větrnými mlýny." [07] Přesvědčení managementu není věcí logiky a rozumu, ale spíše psychologickou hrou, kterou musí bezpečnostní manažeři hrát, aby mohli vyhrát a politiku prosadit. Velice zajímavý článek na toto téma vyšel v ([05], Mgr. Ingrid Matoušková, Psychologie a taktika prosazování investic do informační bezpečnosti ve firemní sféře, červenec-srpen 2004).

Důležitá je i **příprava na samotný proces schvalování.** Podle [07] jsou nejdůležitější následující tři kroky. Prvním z nich je příprava stručného a přehledného dokumentu úderně komentujícího argumenty pro jednotlivé části BP (dokument se označuje jako Důvodové kroky). Cílem tohoto dokumentu je seznámit management s nejdůležitějšími body BP a odpovědět především na otázky typu „Jak jsme na tom teď, které oblasti v politice splňujeme a které ne?", „Pokud zatím politice nevyhovujeme, co musíme udělat proto, abychom to změnili?", „Co bude přijetí politiky znamenat pro naše procesy - jak nás to omezí?", „Jak dlouho to bude trvat a kolik to bude stát?".

Dále při samotné diskuzi je třeba dávat pozor na nepodstatná témata, držet se ohraničeného prostoru - šíře záběru politiky přímo svádí k tomu, aby se diskuze stáčela k nepodstatným věcem a balila na sebe další a další témata.

Podcenit nelze ani přípravu prezentace BP před managementem (povedená či nepovedená prezentace i zde často rozhoduje o výsledku celého snažení).

2.5.2 Vyhlášení bezpečnostní politiky

Po úspěšném schválení a přijetí BP přichází na řadu další úkol - její vyhlášení. Samotný proces vyhlášení BP IS nepředstavuje problém, bude představena stejnou cestou, jako ostatní interní legislativní normy společnosti. Vydání samotné však nestačí, je potřeba zajistit, aby se s politikou seznámili všichni zaměstnanci, a to průkazným způsobem.

Většina zaměstnanců však nemusí znát obsah celého dokumentu, ale pouze ty části, které potřebuje k výkonu svých pracovních funkcí. V případě rozsáhlých bezpečnostních politik, kdy je tento problém opravdu reálný, je užitečné připravit tabulku role / oblasti BP IS. Do polí takové tabulky je pak zaznamenáno, zda je daná oblast pro danou pracovní funkci potřebná.

Takto připravená tabulka pak bude sloužit jako klíč k přípravě školení nebo vytvoření výtahů z BP. Samozřejmostí by mělo být zpřístupnění bezpečnostní politiky na intranetu.

Velice důležitá je také forma samotného podání BP zaměstnancům. Není nic horšího než nudné a ubíjející školení připravené otrocky podle překopírování BP na folie či do powerpointu.

2.5.3 Problémy a chyby při zavádění BP

I v procesu tvorby, schvalování a vyhlašování BP lze najít řadu problémů a chyb. Během schvalovacího procesu se může stát, že díky kompromisům bude nová bezpečnostní politika naprosto nepodobná původnímu návrhu. Problematické pasáže budou vypuštěny nebo přepsány, pravomoci a zodpovědnosti zredukovány na naprosté minimum. Taková BP je pak neúčinná - zobrazuje možná aktuální neutěšený stav, ale neumožňuje dané problémy řešit.

Také může nastat opačný extrém, kdy dojde k vytvoření příliš přísné, až „nereálné“ BP, takové, že ji společnost ve většině ustanovení nevyhovuje. V tomto případě je nutné definovat přechodová období a proces implementace politiky. Pokud se tak nestane postupně, zaměstnanci po seznámení s politikou vnímající realitu výrazně odlišnou od té BP vyžadovanou, budou tuto politiku jako celek zcela ignorovat. Takováto neúcta k vnitřním předpisům pak může vést k ještě mnohem horší situaci, než jaká panovala před zavedením této nové „lepší“ BP.

Jak už jsem zmiňoval v části věnované přijetí BP, velkým kamenem úrazu při snaze o zavedení nové BP může být špatný přístup k managementu. Pokud je managementu předložena příliš rozsáhlá politika – management se nemůže dostatečně podrobně s celým dokumentem seznámit, natož pochopit význam jednotlivých ustanovení. Strach z nereálných závazků a celkových negativních dopadů na výkonnost společnosti může potom proces schvalování velmi zpomalit, nebo i zcela zastavit.

Pokud už se podařilo BP prosadit, je obrovská škoda, kdy z nejrůznějších důvodů je tato politika před většinou zaměstnanců skryta. V mnoha případech se však nejedná o úmysl, ale o podcenění nebo úplné nezvládnutí způsobu komunikace uvnitř společnosti. Sebelepší dokument je v podstatě „k ničemu“, pokud se s ním zaměstnanci neseznámí a pokud se podle něj nebudou řídit.

A jako poslední varování bych uvedl - není dobrým nápadem bez přemýšlení kopírovat politiku jiné firmy, ať už jakkoli kvalitní (výjimku tvoří BP pro malé IS, kdy pro ochranu postačují standardní sady opatření). To, co bez problémů funguje ve firmě jedné, nemusí automaticky plnit potřeby na bezpečnost ve firmě druhé. Vždy je třeba provést analýzu vlastní společnosti a až poté na základě této analýzy začít tvořit novou BP.

2.6 Bezpečnostní normy

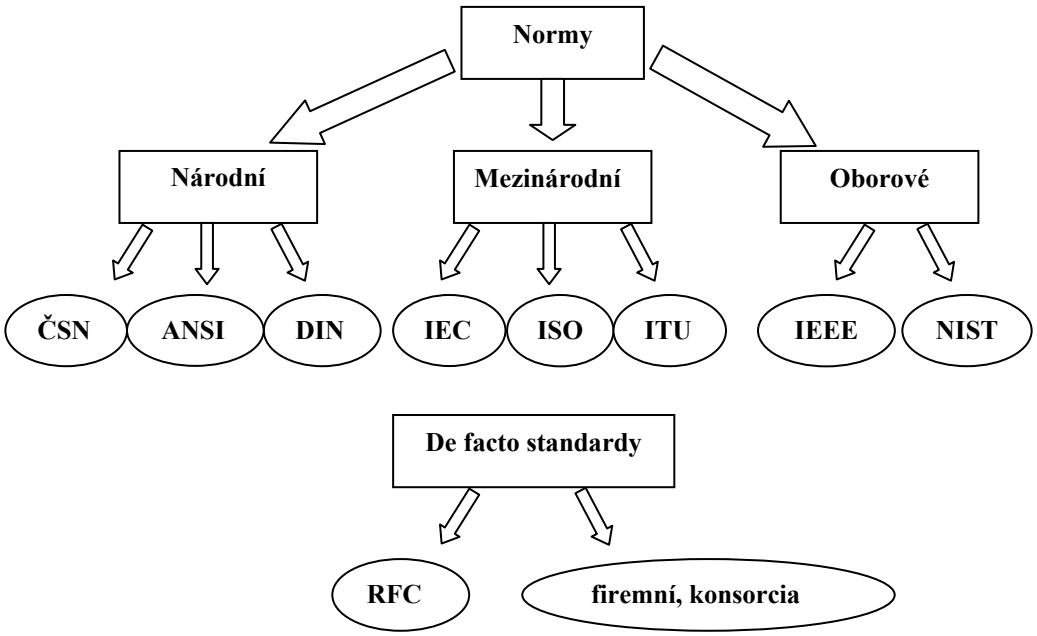
Důvodem vzniku norem v IS/IT je omezení svobody vývojářů a zavedení jakýchsi pravidel do chaosu informačního světa. Normy navíc mohou zajišťovat vzájemnou kompatibilitu, zaručovat danou kvalitu a pomáhají v orientaci ohledně kvalit jednotlivých řešení.

Normu může vydat prakticky kdokoli, horší je to už s přesvědčením ostatních o jejím dodržovaní. Podle českého právního řádu jsou všechny normy pouze doporučené, není-li (speciální případy) stanoveno jinak. Vydáváním norem se zabývá celá řada národních i mezinárodních organizací, tuto činnost vykonává profesionálně, a ve svém oboru platí za uznávané autority. Řada těchto norem je po přeložení do češtiny přebírána i naším normalizačním institutem. Ne všechny normy jsou volně dostupné, např. normy ISO, ANSI i ČSN jsou autorsky chráněné.

Do skupiny nejznámějších mezinárodních norem patří normy vyvíjené v organizacích ISO (International Organization for Standardization), IEC (International Electrotechnical Commission), ITU (International Telecommunication Union). Tyto organizace vydávají i společné normy (ISO/IEC, ISO/ITU-T).

Ale nejenom nadnárodní organizace vydávají světově uznávané normy, existují i národní instituce vydávající normy mezinárodního dosahu. Nejčastěji se lze setkat s normami vydávanými americkým institutem ANSI (American National Standards Institute), německým DIN (Deutche Institut for Normung) aj.. [01]

Schéma číslo 3: Normy, struktura



Zdroj: [01]

Existují také oborové organizace vydávající normy pod záštitou své odborné autority. Mezi nejznámější patří normy vydávané organizací IEEE (Institute of Electrical and Electronic Engineers) a NIST (National Institute of Standards and Technology).

V České republice se normalizací zabývá Český normalizační institut (ČNI). Normy z tohoto institutu mají na sobě označení ČSN (Česká státní norma). V případě, že se jedná o normu převzatou, zůstává normě původní označení a číslování (takže převzatá norma pak bude mít podobu např. ČSN ISO/IEC 13335).

Protože proces schvalování oficiálních norem je poměrně zdlouhavý a vývoj ve světe IS/IT šel mnohem vyšší rychlostí, bylo třeba zavést takzvané de facto standardy - normy, které nebyly nikdy schváleny nějakou oficiální autoritou, které ale byly vytvářeny odborníky (např. vývojová oddělení velkých firem - IBM a spol.) a jsou volně šiřitelné a zveřejněné na Internetu. Kdokoli je může ve svých produktech bezplatně použít, kdokoli je může komentovat a tím popřípadě vyvolat i jejich novelizaci - díky tomuto pravidlu se tyto de facto standardy označují pojmem RFC (Request for Comment).

Zvláštní postavení mezi de facto standardy mají „normy“ vyvíjené a vydávané různými konsorcii. Konsorcium (nebo i významná společnost v oboru) vyvine novou technologii, začne ji implementovat do svých výrobků a snaží se z pozice síly přesvědčit konkurenty, aby tento jejich standard převzali. Pokud se jim to povede, získává obrovský náskok ve vývoji a příjmy vzniklé z následné prodeje. [05], [01]

V přílohách uvádím přehled vybraných norem vztahujících se k bezpečnosti IS.

Certifikát shody

Také je třeba ohlídat, aby systémy postavené na základě nějaké normy, tuto normu skutečně dodržovaly. K tomuto slouží takzvaný certifikát shody - většinou vydávaný nezávislou organizací zaměřenou právě na certifikaci systémů. Náklady na certifikaci pak nese jak výrobce systému (a tento certifikát pak používá při prezentacích svého produktu), tak uživatel (získává jistotu, že systém se bude opravdu chovat podle parametrů uvedených v dané normě). Certifikáty také může vydávat zvláštní asociace tvořená hlavními prosazovateli konkrétní normy (konsorcium firem si zřídí testovací laboratoř, jejímž úkolem bude testování výrobků třetích stran a udělování příslušných certifikátů).

Normy pro hodnocení bezpečnosti IT

Normy pro hodnocení bezpečnosti IS slouží k několika účelům. Zákazník podle těchto norem může z hlediska bezpečnosti porovnávat mezi sebou různé systémy a rozhodnout se pro ten

lépe splňující jeho požadavky. Vývojář se při vývoji systému má čeho „držet“ - tato pravidla mu pomohou zajistit jakousi míru bezpečnosti produktu. A odborní posuzovatelé bezpečnosti systému mají díky těmto normám při ohodnocování ulehčenou práci - stačí jim pouze podle pokynů normy otestovat daný systém a podle dosažených výsledků rozhodnout o ne / splnění požadavků dané normy.

K hodnocení bezpečnosti IS existuje několik široce užívaných norem: asi nejznámější jsou americká kritéria TCSEC (Trusted Computer System Evaluation Criteria, spíše známá jako Oranžová kniha “Orange book”, byla přeložena do češtiny a vydána i u nás: Hospodka B., Karas V.. Kritéria hodnocení zabezpečených počítačových systémů. BEN – technická literatura: Praha. 1994), evropská kritéria ITSEC (Information Technology Security Evaluation Criteria), kanadská kritéria CTCPEC (Canadian Trusted Computer Product Evaluation Criteria) a společná Common Criteria. Více informací o těchto normách lze naleznout na internetových stránkách jim věnovaných, jednotlivá kritéria jsou tam většinou v plném znění s řadou vysvětlujících komentářů.

2.7 Monitoring a audit

Předcházející kapitoly se věnovaly procesu budování zabezpečeného IS s minimalizovanými riziky vzniku bezpečnostních incidentů. Nějaké zbytkové riziko možnosti vzniku bezpečnostního incidentu ale existuje vždy. Proto je třeba vybudovat systém detekčních a nápravných kontrolních mechanismů, které zjistí eventuální výskyt incidentů a přispějí k navrácení systému do původního stavu. Většinu těchto kontrolních mechanismů můžeme shrnout pod tuto kapitolu věnovanou monitoringu a auditu.

V mnoha organizacích je právě monitoring a audit opomíjen a celkové řízení bezpečnosti je tak nekompletní. Jako důvody pro nezavedení těchto kontrolních mechanismů organizace nejčastěji uvádějí, že vlastně nevědí, co by měli monitorovat (nemají přehled o prioritách informací a aktivit); nemají na toto monitorování dostatečnou technickou kapacitu (monitorovací systémy by jim brzdily samotný provoz); nemají na toto monitorovaní dostatek lidských / finančních zdrojů; nemají jasno, kdo by měl v organizaci vyhodnocení provádět.

Pokud se organizace rozhodne pro zavedení monitoringu svého IS, nejprve je třeba stanovit a definovat rozsah monitorovaní. Největší pozornost je třeba věnovat těm oblastem IS, které jsou pro danou organizaci kritické a kterým zároveň hrozí nejvyšší nebezpečí (pravděpodobnost výskytu hrozby, dopad na společnost). Při stanovení rozsahu monitorování nám tedy zřejmě přijde velice vhod analýza rizik (viz. kapitola 2.4). Monitorování by dále mělo postihnout jak neúmyslné hrozby, tak hrozby úmyslné.

Po ujasnění rozsahu monitorování a práv a povinností zainteresovaných osob je třeba samotný monitorovací proces zahájit. K tomu je třeba nejprve implementovat sledovací zařízení.

Monitorovací prostředky

Monitorovací prostředky lze rozdělit do dvou základních skupin na technické prostředky a manuální procesy. Do technických prostředků patří například sledování údajů o přihlášení a odhlášení uživatele, neautorizovaných pokusech o přihlášení do systému, vytížení systémových zdrojů, záznamy spouštění jistých služeb, pokusy o neautorizované využití služeb systému, záznamy rizikových událostí specifických pro daný systém, atd.. Velká část technických prostředků pro tyto auditní záznamy je obsažena ve službách OS (např. Event Log v MS Windows), pro jiné je nutný speciální nástroj. Do manuálních procesů například můžeme zařadit postupy vyhodnocování auditních záznamů včetně vyhodnocování bezpečnostních incidentů.

Jakmile je monitorovací proces funkční, je třeba začít s vyhodnocováním výsledků - bez vyhodnocování samotné monitorování ztrácí smysl.

Auditní záznamy

Záznamy pro zpětné sledování funkcí systému, nedocenitelné při vyhodnocování bezpečnostních incidentů a zjišťování příčin, zodpovědností a nápravných opatření pro zabránění opakování této situace. Každý bezpečný IS by měl být schopen minimálně uchovávat tyto informace: datum a čas události, přihlášeného uživatele, počítač, provedenou akci s co nejpodrobnějším popisem, úspěšnost provedené akce (např. i neúspěšné pokusy o přihlášení).

Bezpečnostní audit

I přes dobře nastavené provozní mechanismy pro monitorování informační bezpečnosti je třeba, aby byly prováděny interní / nezávislé audity klíčových prvků a procesů informačních technologií pro ujištění, že zavedené bezpečnostní kontrolní a monitorovací mechanismy fungují v daném prostředí odpovídajícím způsobem. Mnoho organizací využívá pro tyto aktivity spojené s nezávislým posouzením informační bezpečnosti rovněž externí společnosti – buď z důvodů nedostatečného počtu interních auditorů na úplnou komplexní kontrolu zavedených bezpečnostních opatření, nebo, když je třeba o určitých aspektech informační bezpečnosti podat zprávu třetím stranám.

2.7.1 Penetrační testování

Na rozdíl od většiny ostatních způsobů monitorování, které jsou založeny na analýze událostí minulých, penetrační testování je zaměřeno na aktivní odhalování bezpečnostních slabin. Penetrační testy dělíme podle polohy „útočníka“ vzhledem k systému na **vnitřní a vnější.**

Při vnějších penetračních testech se bezpečnostní specialisté změní na hackery a pokusí se do testovaného IS proniknout. Tyto vnější testy se mohou konat v podstatě odkudkoli (většinou sídlo bezpečnostní firmy).

Vnitřní penetrační testy jsou uskutečňovány zevnitř z firemní sítě, simulují chování nespokojeného zaměstnance / osoby, která získala fyzický přístup k terminálu IS.

Útoky prováděny při vnějších / vnitřních penetračních testech končí kompromitací IS (získání neoprávněného přístupu, popř. získání administrátorského účtu).

Penetrační testování patří do rodiny takzvaných „technických testů“. Tyto testy bývají často součástí analýzy rizik IS. Výstupem technických testů je podrobná písemná zpráva, která popisuje nalezené zranitelnosti, rizika s odhadem jejich míry dopadu. Ke každému identifikovanému riziku je podáno doporučení na jeho odstranění, případně snížení na požadovanou úroveň. Mezi další technické testy patří například analýza konfigurace systému detekce / prevence průniku, analýza konfigurace firewallů, aktivních síťových prvků, operačních systémů na serverech, systému zálohování, bezpečnosti a spolehlivosti speciálních systémů a aplikací apod..

2.8 Ochrana informací a legislativa ČR v rámci EU

Zákonů a vyhlášek věnujících se nějakým způsobem ochraně informací existuje v České republice mnoho. Liší se oblastí své působnosti, svými cíly, aspekty bezpečnosti, které berou do úvahy, a v neposlední řadě se také liší tím, jak podrobně a zda vůbec se zabývají otázkami řešení.

Z iniciativy EU v rámci harmonizace legislativ nově přistupujících zemí (v tomto případě v přístupu k ochraně osobních údajů na jejím území - přesněji k ochraně osob s ohledem na automatizované zpracování osobních údajů a také směrnicí č. 95/46/ES o ochraně osob se zřetelem na zpracování osobních dat a o volném pohybu takových dat) byl již v roce 2000 přijat nový zákon č. 101/2000 Sb. na ochranu osobních údajů. Zákon upravuje ochranu osobních údajů o fyzických osobách, práva a povinnosti při zpracování těchto údajů a stanoví podmínky, za nichž se uskutečňuje jejich předávání do jiných států. Tento zákon nahradil dosavadní zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech. Dalších zákonů týkajících se ochrany informací, které by byly ze strany EU takto zvýrazňovány, si nejsem vědom.

V práci není dostatek prostoru na rozepisování obsahu jednotlivých zákonů a vyhlášek, rád bych zde alespoň vyjmenoval ty nejdůležitější. Plná znění těchto zákonů a vyhlášek lze nalézt buď na stránkách jednotlivých státních úřadů mající dané dokumenty na svědomí (Národní bezpečnostní úřad - http://www.nbu.cz/, Úřad pro ochranu osobních údajů - http://www.uoou.cz/, Ministerstvo informatiky ČR - http://www.micr.cz aj.), nebo v mnohdy mnohem přehlednější podobě na informačních portálech určených pro podnikatele (např. http://business.center.cz/, http://www.businessinfo.cz).

Vybrané zákony a vyhlášky zaměřené na ochranu informací

Zákon č. 513/1991 Sb., Obchodní zákoník (§ 17 obchodní tajemství),

Zákon č. 148/1998 Sb. o ochraně utajovaných skutečností ,

Zákon č. 101/2000 Sb. o ochraně osobních údajů,

Zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon),

Zákon č. 151/2000 Sb. o telekomunikacích, příp. přijatý návrh zákona o elektronických komunikacích,

Zákon č. 227/2000 Sb. o elektronickém podpisu,

Zákon č. 480/2004 Sb. o některých službách informační společnosti,

Zákon č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti,

Vyhláška č. 56/1999 Sb. o zajištění bezpečnosti informačních systémů nakládajících s utajovanými skutečnostmi, provádění jejich certifikace a náležitostech certifikátu,

Vyhláška č. 136/2001 Sb. o zajištění kryptografické ochrany utajovaných skutečností, provádění certifikace kryptografických prostředků a náležitostech certifikátu,

Vyhláška č. 366/2001 Sb. o upřesnění podmínek stanovených v § 6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu,

Vyhláška č. 137/2003 Sb. o podrobnostech stanovení a označení stupně utajení a o zajištění administrativní bezpečnosti,

Vyhláška č. 339/1999 Sb. o objektové bezpečnosti.

3. Vybraná současná bezpečnostní rizika

V této části bych rád představil některá aktuální bezpečnostní rizika, se kterými se bezpečnostní specialisté potýkají. Slovo aktuální není v tomto případě vázáno k časovému horizontu, ale k problémům existujících v současném uspořádání informačního světa. Zdrojem pro výběr vhodných témat pro mne v tomto případě byla periodika zabývající se problematikou bezpečnosti (a to nejenom informační) - jak podoby tištěné [04], [10], tak pro nejaktuálnější informace, podoby elektronické [I-01], [I-03], [I-04].

3.1 Teorie útoků

Ještě předtím, než se budu věnovat konkrétním bezpečnostním rizikům, bylo by dobré alespoň ve zkratce zmínit teorii útoků. Útokem (bezpečnostním incidentem) rozumíme buďto úmyslné nebo neúmyslné uskutečnění akce (využití zranitelného místa), jejímž výsledkem je škoda na aktivech. Útoky se dají dělit podle zaměření (HW, SW), způsobené škody (ne / významné), úmyslu (ne / úmyslné), přístupu (aktivní x pasivní), úspěšnosti (ne / úspěšné), místa původu (z vnějšku / zevnitř), záleží na úhlu pohledu a na tom, čeho se snažíme daným dělením dosáhnout.

Útočit lze **přerušením, odposlechem, změnou a přidáním hodnoty.** Útoky přerušením představují aktivní útoky (aktivně zasahuje do komunikace / běhu IS) na dostupnost služeb (ztráta, znepřístupnění, poškození aktiva, porucha periférie, vymazání programu / dat, porucha v operačním systému / programu, přetížení systému / jeho části - takzvané Dos, dDoS útoky). Útočníkovi v tomto případě jde o znemožnění komunikace – nedokáže data odposlechnout, modifikovat ve svůj prospěch, alespoň je může modifikovat, zničit či zabránit v přístupu k nim. K těmto útokům útočníci využívají hlavně škodlivý software, přesněji počítačové viry a červy.

Při útoku odposlechem dochází k pasivnímu útoku (nezasahuje do komunikace / běhu IS) na důvěrnost dat, útočníci se snaží o získání dat, ke kterým by se oficiální cestou nedostali (neoprávněné okopírování programu / dat). Nebezpečí pasivních útoků spočívá v nesnadné detekci odposlechů. Pasivní útoky lze realizovat přes malware (trojské koně, spyware, červy, keyloggery), fyzické odposlechy přenosových médií. Důvěrné informace lze ale také získat přes sociotechniku, či kombinací sociotechniky a technických prostředků (spam-hoaxy, phishing, pharming - aktivní útoky změnou a přidáním hodnoty, viz. dále), případně „útokem“ na jejich neelektronickou podobu (papírové dokumenty v kanceláři, v popelnici před firmou apod.).

Útoky změnou a přidáním hodnoty představují aktivní útok na integritu / autenticitu dat, neautorizovaný subjekt zasáhne do aktiva (změna uložených / přenášených dat, přidání funkce do programu, změna čísla účtu, částky, emailu atd.). Tato situace je velice nepříjemná, pokud

komunikující strany (systémy) nejsou schopny tuto modifikaci nějak detekovat. Ne vždy je cílem modifikovat přenášená data, někdy je výhodnější postavit se do role odesílatele těchto dat. Využitím je snaha o podvržení autentizační informace, kdy se útočník snaží ukrást cizí identitu, kterou pak zneužije pro vlastní potřebu. Nyní se už můžeme podívat na jednotlivé bezpečnostní hrozby.

3.2 Škodlivý software

Škodlivý software, jinak také přezdívaný malware (malicious software), představuje programy, nebo části programového kódu, které bez vědomí uživatele provádějí činnosti, jejichž účelem je způsobit škodu / obtíže.

Mezi jeho nejstarší představitele patří počítačové viry. V poslední době však podle IT specialistů mnohem větší problém namísto klasických virů představují trojské koně (hlavně jejich speciální odnož - spyware) a počítačoví červi. Pro úplnost jsem do této kapitoly o škodlivém software ještě přidal alespoň základní informace o Dialerech a Keyloggerech.

3.2.1 Viry, Červi, Trojské koně

Počítačové viry

Podobné skutečným virům, přenášejí se a přežívají pomocí napadeného souboru (hostitele). Infikují jiné programy, paměťová média. Do svého šíření aktivně nezasahují. Napadnou vybrané soubory a čekají, až budou přeneseny na jiný počítač a spuštěny.

Viry rozlišujeme podle míst a typu souborů, které pro své šíření používají. **Souborové viry** napadají spustitelné soubory, anebo soubory obsahující alespoň zčásti spustitelný kód. Speciálním případem souborových virů jsou **makroviry** (pro dokumenty MS Office, zneužívají zavedeného programovacího jazyku pro tvorbu maker usnadňujících práci). **Bootviry** se šíří prostřednictvím zaváděcích sektorů. Většina virů se dokáže šířit více způsoby – například kombinací boot sektoru a souborů.

Počítačové viry se projevují různě. Zpomalují, destabilizují systém, šifrují / mažou data, zabírají místo, vypisují různé obtěžující hlášky atd.. Tím „nejlepším“ možným projevem je nějaká snadno rozpoznatelná činnost. Nejhorší viry jsou ty, které postupně pomalu napadají celý systém, přehazují písmenka a slova v textových souborech a dají o sobě zřetelně vědět až tehdy, když už jsou takřka na každé záložní kopii a jejich odstranění je velice obtížné až nemožné.

Také existují viry škodící pouze po splnění určitých podmínek, nejčastěji po nějakém datu, počtu spuštění atd., cílem znovu snaha o nakažení co největšího počtu PC bez upozorňujícího projevu.

Jako obrana před počítačovými viry slouží antivirové programy (4.1), firewally (4.2).

Červi

Pracují na nižší síťové vrstvě než viry. Nešíří se formou infikovaných souborů, ale síťových paketů. Tyto pakety vycházejí z již napadených systémů na další počítače v síti Internet (náhodně, určité klíče). Pokud tento paket narazí na OS s tou „vhodnou“ bezpečnostní dírou, dojde k jeho infekci a dalšímu šíření infikovaných paketů. Šíření červa je tedy postaveno na bezpečnostních dírách SW, úspěšnost šíření pak na rozšířenosti tohoto SW (OS, poštovní klienti, IM programy atd.). Pojem “červ“ je často spojován i s typem infiltrace šířící se elektronickou poštou.

Napadené systémy se mohou chovat různě. Může dojít k smazání dat, opakovaným restartům (Lovsan / Blaster), shazováním jistých systémových procesů (Sasser). Vedlejším efektem těchto červů při opravdu masivním rozšíření může být zahlcení sítě (jak lokální tak i celého Internetu).

Obranou proti těmto červům jsou jednak antivirové programy a jejich moduly pro ochranu poštovních klientů, firewally, bezpečnostní záplaty pro odpovídající klienty, správná nastavení klientů (přístup k zobrazování příloh, interpretace dopisů v HTML formátu apod.).

Trojské koně

Destruktivní programy, maskující se jako neškodná a užitečná aplikace (antivirový program, nová verze nějakého oblíbeného programu, atd. proto trojské koně). Tento program potom bez vědomí uživatele provádí nekalou činnost - hlídá stisky jednotlivých kláves a ty pak odesílá na vybrané emailové adresy, ničí data na disku, otevře zadní vrátka do systému umožňující jeho převzetí, vpustí do systému vir uložený ve vlastním kódu, pokusí se stáhnout nějaký vir z URL, zneužije napadený počítač pro odesílání spamu, spustí FTP server a umožní volné stahování souborů, zapojí počítač do „sítě“ pro DDOS útoky atd..

Narozdíl od virů nejsou trojské koně schopny rozmnožování (sebereplikace) a infikování dalších souborů. Obrana stejná jako v případě virů. Speciální verzí trojského koně je spyware, o něm ještě bude řeč dále.

Seznam nejznámějších trojských koňů s jejich podrobným popisem je k dispozici na http://www.glocksoft.com/trojan_port.htm.

Poznámky na závěr:

1) I pokud není na počítači nainstalován žádný antivirový program, lze pouhým obezřetným chováním předejít nákaze od mnoha druhů malware (včetně spyware a dialerů, o kterých je řeč dále):

- při zacházení s elektronickou poštou je hlavně nutné dávat pozor na elektronické přílohy, které mnoho z těchto druhů software využívá pro napadení počítače (většinou se jedná o dopisy s aktuálními tématy či „zajímavými" fotkami celebrit - v poslední době například fotky zesnulého papeže Jana Pavla II., email s informacemi o ptačí chřipce, fotografie ze zemětřesení atd.).

Dalšími oblíbenými triky kromě příloh jsou: falšování adresy odesílatele, nepravdivé ujištění, že zpráva byla zkontrolována antivirovým programem, dvojité přípony apod..

- při brouzdání po Internetu na méně důvěryhodných stránkách dávat pozor na jakékoli dialogy, popřípadě v MS IE vypnout Active X, javascripty, apod.
- před instalací nějakých freewarových / sharewarových prográmků je dobré kromě oficiálních stránek navštívit nějaké hromadné download servery, kde v diskuzi pod daným programem by bylo na přítomnost nějakého malware jistě upozorněno.

2) Na počátku roku 2004 také nastala situace dosud nemající v historii virů a antivirového boje obdoby. Během několika dnů se objevily desítky verzí emailových virů (červů) Netsky, Bagle, MyDoom. Každý z těchto virů napáchal menší epidemii, ale co je hlavní, bylo to, že tyto viry mezi sebou navzájem sváděli bitvu. Na napadených počítačích se snažily najít „konkurenční" malware a ten pak mazaly a autoři těchto virů si navzájem v kódech viru posílali slovní urážky (pokud se verze virů poskládaly dohromady, tak to téměř vypadalo jako rozhovor).

3) Rok 2004 se vůbec zdá být zajímavým „virovým" rokem, protože v tomtéž roce se také objevili první viry pro mobilní aplikace. Pomocí Bluetooth se po zařízeních s OS Symbian EPOC Series 60 šířil červ Cabir a o pár týdnů potom byl zaznamenám první vir pro platformu Pocket PC (Windows CE) - Duts.

Ani jeden z těchto kódů nebyl škodlivý, ani nijak reálně nebezpečný (Cabir se snažil rozeslat mezi další přístroje a tím rychle vybil baterku, Duts se dotázal, zda si uživatel přeje své Pocket PC infikovat), nedošlo ani k jejich většímu rozšíření (pouze lokální epidemie, například stadion v Helsinkách na atletickém mistrovství světa) ale naznačily, že mobilní platformy nejsou bezpečné a v budoucnu nás čeká mnoho nemilých překvapení.

4) Podle Y. Kasperskyho (Kaspersky Lab) se také blíží doba, kdy počítačové viry napadnou a ovládnou automobily. Zhoubné kódy již nyní útočí přes rozhraní Bluetooth, jež je využíváno

k přenosu dat z mobilů či MP3 přehrávačů do palubní elektroniky. Podle některých scénářů by takové napadení vozidla mohlo mít za důsledek ztrátu kontroly nad výkonem motoru, navigací nebo použitím multimediálních systémů. "Stále byste však měli mít možnost řídit vozidlo vlastními silami," dodal Guido Sandrian ze společnosti Symantec. Jedním z prvních případů, kdy se do vozidla dostal virus, byla Toyota Lexus LX470. Pomocí Bluetooth rozhraní byl napaden GPS systém (navigační systém) tohoto automobilu.

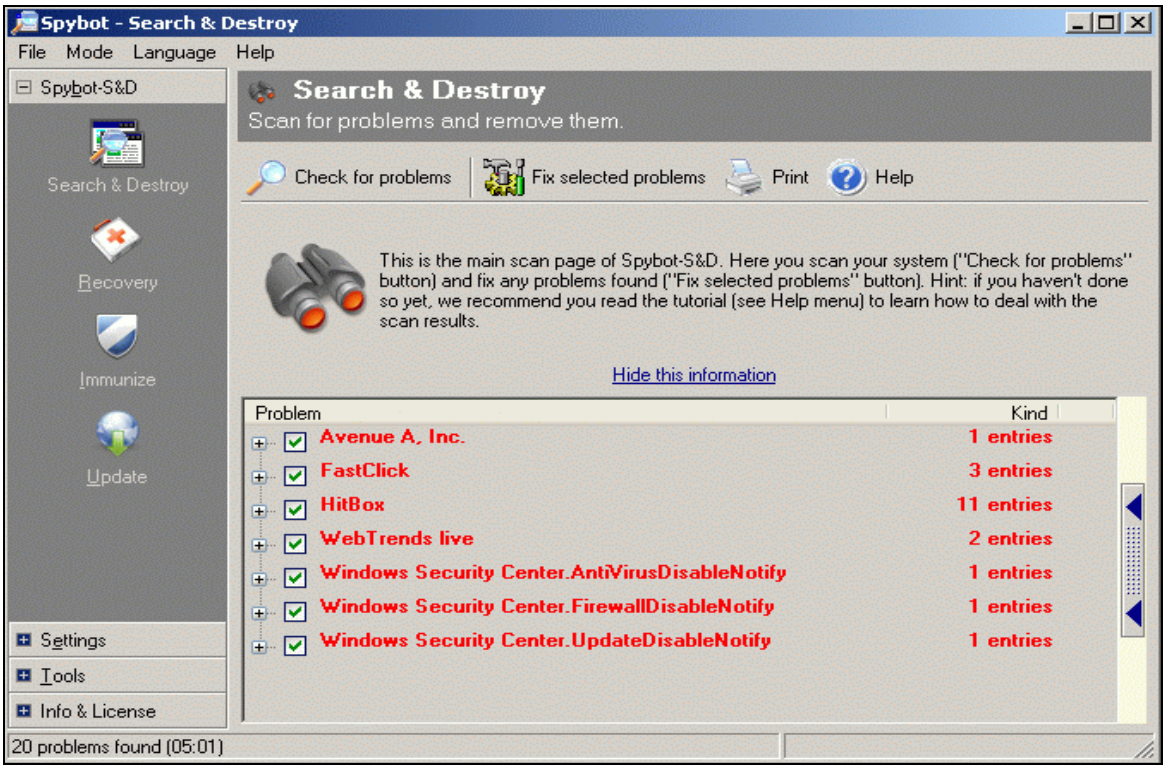
5) Pro aktuální informace o virových nebezpečích šířících se prostřednictvím elektronické pošty vznikl u nás projekt "Virový radar on-line", adresa je http://www.virovyradar.cz/ .

3.2.2 Spyware

Název odvozený od anglického SPY (sledovat, slídit, pátrat). Cílem takto označovaných programů není nic jiného, než získávat informace (statistiky o navštívených stránkách, instalovaném SW, konfiguraci PC atd.) bez vědomí jeho uživatele. Jako odůvodnění tohoto „špehování“ tvůrci spyware uvádějí snahu o zjištění potřeb a zájmů uživatele (jakýsi marketingový průzkum). Nikdo ale nemůže zaručit, co se s těmito daty stane dále, navíc tato technologie může být snadno zneužita pro vynášení opravu citlivých údajů.

Spyware bývá většinou obsažen v užitečných programech šířených pod licencí shareware, freeware. Na Internetu jsou k dispozici programy na odstranění těchto programů, pak ale i samotný „hostitelský“ užitečný program zpravidla přestává fungovat. Existují ale i druhy spyware využívající nezabezpečenosti webového prohlížeče (zatím hlavně MS IE, s rostoucím počtem uživatelů alternativních prohlížečů se ale dá očekávat snaha tvůrců těchto programů o rozšíření jejich působnosti) a nepozornosti uživatelů, kteří bezmyšlenkovitě potvrzují dialogová okna bez znalosti jejich obsahu.

Obrázek číslo 1: Antispywarový program Spybot S&D, výsledky testu



Zdroj: Vlastní tvorba

Obranou je antivirový program schopný vyhledávat spyware, správně nakonfigurovaný a záplatovaný webový prohlížeč, vhodné je použít některý z volně šiřitelných nástrojů pro vyhledávání a ničení spyware (Ad-Aware, Spybot S&D, SpywareBlaster a jiné), neinstalování podezřelých aplikací, při brouzdání po Internetu pozorné sledování předkládaných dialogů a jako vždy záplatování.

Poznámky na závěr:

1) Podle statistik přes 90 procent počítačů obsahuje alespoň jeden exemplář nějakého spyware. Přičemž ale průměrné číslo počtu rozdílných kódů spyware na jeden počítač je 28! [10]

2) Pro další informace o těchto programech doporučuji navštívit české stánky na http://spyware.cz.

3.2.3 Adware

Software, znepříjemňující práci s PC reklamou. Nejméně škodlivé adware programy jsou stejně jako v případě spyware vloženy do aplikací, kde viditelně zobrazují aktuální reklamní

bannery stahované z Internetu – za to bývá uživatelovi zpřístupněna celá řada funkcí, jinak dostupná pouze u placené verze. Uživatelé jsou většinou předem informováni přes licenční ujednání o tom, že si instalují program, jehož vývoj je financovaný reklamou.

Horším případem jsou nechtěné adware programy natažené do počítače během brouzdání po Internetu bez vědomí uživatele – tyto programy pak při prohlížení dalších stránek samovolně vyskakují reklamní okna, přesměrovávají domovskou stránku prohlížeče, zvýrazňují v textu stránek jistá pro ně „klíčová“ slova (názvy / typy produktů atd.) a k nim vyskakují tabulky s možností objednání apod..

K odstranění a obraně proti adware slouží většinou stejné programy a postupy jako v případě spyware. Už jsem se ale setkal s několika případy, kdy byl systém a jeho hlavní soubory tak „prolezlý“ těmito programy, že po odstranění byl nestabilní / přestal fungovat úplně. Jediným řešením pak byla kompletní reinstalace.

3.2.4 Dialery

V dnešní době již přestávají být problémem, přesto je ale pro úplnost třeba je zmínit. Dialery jsou programy, které změní způsob připojení k Internetu po modemu. Místo běžného telefonního čísla pro internetové připojení přesměruje vytáčení na čísla se zvláštním tarifem desítek korun za minutu. Dost často se toto přepojení dělo bez vědomí uživatele, stačilo se špatně zabezpečeným prohlížečem navštívit nějaké nedůvěryhodné stránky. V momentě, kdy uživatel tuto změnu zjistil (většinou se tak stalo až po přijití výpisu od Českého Telecomu, a.s.), již byla škoda napáchána.

Nemusí se ale vždy jednat o ilegální program, mohou sloužit i jako způsob zpoplatnění určité služby.

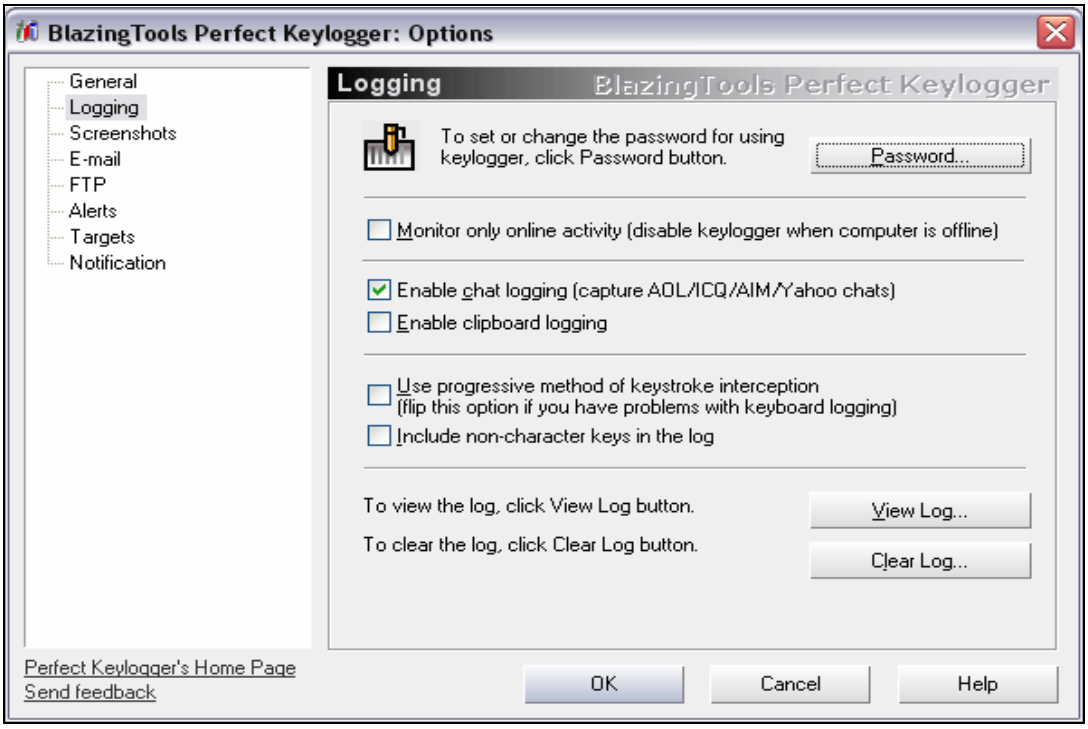
K obraně slouží programy pro hlídání způsobu vytáčeného připojení, detekci dialerů (např. Connection Meter, http://www.conmet.cz/) či zablokování těchto linek.

3.2.5 Keyloggery

Nejedná se přímo o škodlivý software, řada těchto produktů je plně komerčních, ale je dobré se o nich také zmínit (někteří autoři je řadí pod klasické trojské koně). Jak už název napovídá, primární činností keyloggerů je zaznamenávání stisknutých kláves. Pokročilejší verze obsahují více funkcí, jako např. pravidelné / selektivní (podle názvu okna aplikace) sejmutí aktuální obrazovky, zaznamenávání obou stran dialogu přes IM programy, zaznamenávání kliků myši na ikony, obsahu schránek pro kopírování, seznamu navštívených stránek atd.. Takto získané

údaje tyto programy buďto nechávají uložené na lokálním počítači, nebo je jsou schopny rozesílat dál po síti, na FTP, emailem.

Obrázek číslo 2: Perfect Keylogger, ukázka nastavení



Zdroj: http://www.blazingtools.com

Tyto programy pracují zcela skrytě, nenajdete je ani ve spuštěných procesech. K jejich odhalení je třeba využít speciálního SW (Spy Sweeper, Anti spy atd.).

„Využití“ keyloggerů je široké. Na hranici zákona bude sledování zaměstnanců v práci, zda se nevěnují soukromým záležitostem (emaily, SMS, psaní dokumentů). Mohou sloužit ale i k prospěšné činnosti - nechat si sledovat domácí PC, zda se na něm v nepřítomnosti majitele nedějí nepřístojnosti (např. sledování dětí, zda se nezajímají o věci mimo jejich věkovou kategorii).

Keylogger ale zrovna tak snadno na počítač může dát osoba třetí, která se tím dozví o každém úhozu kláves majitele daného počítače. Rizika z toho vyplývající jistě není třeba podrobněji rozebírat. Zvláštní pozornost tomuto typu programů je nutno věnovat při používaní veřejně přístupných počítačů (školní počítače, internetové kavárny).

3.3 Spamming a Spam

Spamming je jednou z nových forem zneužití elektronické komunikace. Spam je nevyžádaná elektronická pošta (junk mail papírová). Provozovat spamming znamená zaplavovat internet mnoha exempláři jedné a téže zprávy ve snaze vnutit ji lidem, kteří by jinak takovou zprávu vůbec přijmout nechtěli. Většina spamů jsou obchodně zaměřené nabídky, nebo nabídky pochybných produktů.

Spamming zneužívá distribučních systémů dnešních počítačových sítí (odeslání konkrétní zprávy k jedinému příjemci / skupině dá stejně práce, původně vyvinuto pro skupinové diskuze mezi osobami zainteresovanými). **Představuje takovou hromadnou distribuci zpráv (texty, přílohy), která je iniciována pouze jednostranně, sleduje výhradně jednostranné zájmy a je ostatním stranám vnucována.**

Hlavním problémem spammingu je fakt, že tyto výše zmíněné aktivity nutí do spolupráce i další strany - příjemce spamu. Ti potom musí nedobrovolně vykonávat čas beroucí činnosti, jako rozpoznávat legitimnosti nabídek, mazat nevyžádané emaily a přitom se i finančně spolupodílet na nákladech (náklady na distribuční služby nesou všichni zúčastnění: příjemce, odesílatel, poskytovatel připojení) na přenos něčeho, co vůbec nechtějí - spamming tak zneužívá kolektivního způsobu financování, tím se zásadně odlišuje od rozesílání nevyžádaných listovních zásilek, kde veškeré náklady nese pouze iniciátor kampaně.

K tomu všemu ještě spamming omezuje uživatele ve svých právech (nemohou využít to, co si nakoupili tak, jak by bylo jinak obvyklé) a následně jim mohou vznikat nepřímé škody (díky přeplněné schránce neobdrží důležitý email, díky chybě nutného spamového filtru skončí žádoucí emaily ve spam koši, stahování nechtěné pošty čerpá z datových limitů na připojení apod.).

Dělení spamu:

Podle obsahu dělíme spam na zásilky reklamního charakteru (inzerující produkty a služby), návody (na rychlé zbohatnutí, zázračné léčebné metody a postupy), řetězové dopisy, recese, urážky, pomluvy, diskreditace a další.

Spamovat se dá elektronickou poštou, prostřednictvím offline / online diskusních skupin (News / IRC), přes SMS do mobilů, IM.

Příjemci spamů jsou buďto adresováni přímo (konkrétní předem známé adresy získané např. z www, zcizené / odkoupené databáze od třetí osoby (výrobce spyware), monitoringem diskusí apod.) nebo nepřímo (spam rozeslán na určitý distribuční kanál a příjemcem se stanou všichni jeho uživatelé).

Proč je spam škodlivý?

Spam je označován za bezpečnostní riziko z několika důvodů. Tím nejviditelnějším je obtěžování uživatele, který musí každý takový email zkontrolovat a následně na něj zareagovat (smazat), čímž věnuje svůj čas, um a energii na neproduktivní aktivity (zcizování zdrojů), které by jinak nemusel vykonávat. Zneužívá osobních údajů (elektronických adres) k jiným účelům, než k jakým jsou jejich vlastníky určeny. Dále spam omezuje funkčnost komunikačních systémů, protože svým rozesíláním spotřebovává určitou část kapacity přenosového média (extrémním případem je zahlcení linky, zaplnění emailové schránky). K tomu spam vytěžuje i další zdroje - přenosovou kapacitu, diskový prostor, výpočetní kapacitu atd. (spotřeba lineárně roste s množstvím spamů). A posledním často uváděným důvodem je již zmiňované zneužívání kolektivního financování distribučních kanálů.

Jak se spamu bránit?

Spam lze omezit na území státu zákonem, který danou problematiku upraví (u nás je tímto zákonem zákon č.480/2004 Sb. o některých službách informační společnosti). Bohužel tento zákon je aplikovatelný jenom na území státu, který tento zákon vydal, přičemž většina spammerů svoji činnost provozuje ze zemí, kde spamování zákonem stíháno není.

Další možností omezení je použitím technických prostředků (filtrování a následná eliminace zpráv představující spamy) - o nich pojednává kapitola „4.3 Antispamové programy“.

Poslední možností spadající podle mě ale prozatím spíše do říše snů je bojovat proti spammingu cestou osvěty a vytvořit takovou společenskou atmosféru, která by potenciálním i aktuálním spammerům vzala motivaci.

3.3.1 Hoax

Anglické slovo Hoax znamená v překladu falešnou zprávu, mystifikaci, novinářskou kachnu, podvod, poplašnou zprávu, smyšlenku, výmysl, žert, kanadský žertík. V počítačové terminologii jako Hoax označujeme zprávu, která obvykle varuje před neexistujícím nebezpečným virem, jiným nebezpečím, falešnou prosbou o pomoc, fámami o mobilních telefonech, peticích a výzvách. Dalšími typy Hoaxů jsou podvodné emaily, pyramidové hry, řetězové dopisy štěstí a žertovné zprávy.

Hoax má se spamem mnoho společných rysů. Jedná se o nevyžádanou zprávu, zpravidla obtěžující, která jen zbytečně zatěžuje linky. Šíření Hoaxů je však narozdíl od spamů zcela závislé na uživatelích, kteří takovou zprávu emailem obdrží. Někteří se mohou pokusit „varovat“

/ „informovat“ další kamarády či spolupracovníky a jednoduše jim poplašnou zprávu přeposlat (forwardovat). Tím vzniká proces šíření.

Neexistuje univerzální návod jak rozeznat Hoaxy. Nicméně, pokud dostanete do emailu dopis s nějakým „podezřelým“ obsahem, kde na konci zpráva obsahuje výzvu k hromadnému rozeslání na další adresy, je to s největší pravděpodobností Hoax. Pokud podobnou zprávu obdržíte, doporučuji navštívit stránky se seznamy již identifikovaných Hoaxů a určitě tam nějakou podobnou zprávu naleznete. Nejméně šťastným řešením je přeposlání těchto zpráv všem lidem z kontakt listu (můžete tím u dosti lidí ztratit na důvěryhodnosti), a je třeba dát pozor, ať při případném rozesílání dál nedojde k prozrazení nějaké důvěrné informace (emaily se šíří řetězově a obsahují v sobě spoustu předešlých adres, některé žádají o poslání osobních údajů atd. - ráj pro spammery). A nikdy není jisté, kdo bude dané emaily číst po vás.

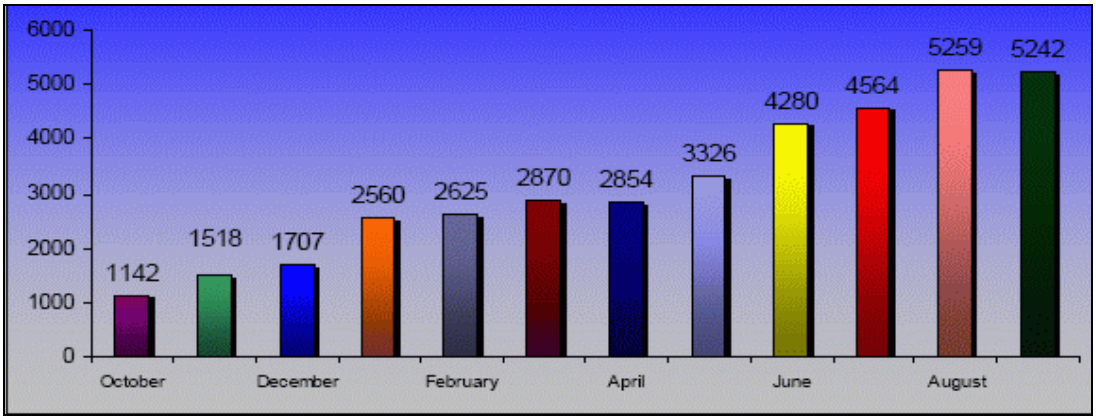
Pokud mi někdo zašle nějaký druh takového dopisu, nebo zprávu po ICQ (například nechvalně známá fáma - hrozí placené ICQ, rozešli dál a zmodrá ti kytička a nebudeš nic platit apod.), tak daný dopis či zprávu smažu a odesílatele odkazuji na kvalitní českou stránku zaměřenou právě na problematiku Hoaxů - http://www.hoax.cz.

3.4 Phishing a pharming

3.4.1 Phishing

Ač se o phishingu mluví až v posledních několika letech, nejedná se v podstatě o nic nového. „Stejné“ podvody existují již mnoho let a kořeny má tato metoda ještě před vznikem počítačů. Podvodníci tyto podvody páchali celá léta po telefonu a nazývali je sociálním inženýrstvím. Teď se jejich novým nástrojem stal spam a podvržené webové stránky. [I-14]

Obrázek číslo 3: Počet nově objevených falešných prezentací říjen 2004 – září 2005



Zdroj: http://antiphishing.org (20.12.05)

Phishing = fishing (rybaření) + phreaking (předchůdce hackingu - nabourávání telefonních služeb), česky se poměrně vžívá název „rhybolov“ (opravdu rybolov připomíná, v podstatě jde o rozhození návnady v podobě lživých emailů a čekání, kdo se chytí) označuje metodu používanou za účelem získávání jmen a hesel ke službám, osobních údajů, čísel účtů atd.. K odcizování údajů podvodníci používají hlavně podvržené a zfalšované emaily, které uživatele (zákazníky nějaké služby – finanční sektor, ISP, eBay, humanitární organizace, portály atd.) odvedou na falešné webové prezentace (které se ovšem tváří, že jsou v pořádku), kde pak z těchto uživatelů pod nejrůznějším účelem lákají dané údaje, snaží se o zavedení trojského koně (hlavně keyloggery a zadní vrátka) apod..

Díky tomu, že tito podvodníci volí známé obchodní značky, mají celkem slušnou šanci oslovit někoho, kdo na tuto zfalšovanou výzvu odpoví (nemluvě o situaci, kdy se provalí databáze klientů s adresami) a následně dané údaje vyzradí. Podle serveru http://www.antiphishing.org/ se přitom těmto útočníkům jejich podvody celkem daří (5 procent oslovených útoku podlehne). Což je při jednoduchosti a průhlednosti tohoto triku poměrně zarážející. Přičemž počet těchto útoků neustále roste. Jen za letošní září bylo nahlášeno 13,562 unikátních phishing emailů a zjištěno přes 5242 unikátních falešných webových prezentací, přičemž bylo zneužito názvu 106ti obchodních značek. [I-13]

Technická stránka

Aby byl phishing úspěšný, nelze se spoléhat jen na sociotechniku (email a okopírovaný vzhled stránek). Přemlouvání by bylo k ničemu, kdyby vás podvodníci nějakým způsobem nedokázali přesvědčit, že se opravdu nacházíte na legitimní stránce (aneb těžko by někdo uvěřil přihlášení do eBanky pod adresou neconeco.webzdarma.cz). K tomuto přidání „puncu pravosti“ podvodníkům slouží následující metody:

- zfalšování hlavičky emailu: změna kolonky OD: přes speciální nástroje, PHP, telnet atd..

obrana: prohlédnutí hlavičky emailu a pole received,

- využití podobností: spoléhá na nepozornost uživatelů, podobně vypadající názvy domén, může vypadat velice opravdově (paypal.com a paypa1.com, jednou „el“ a jednou číslice apod.), přímo vést na stránky pravé.

obrana: a) email informuje o nové doméně - projet doménu databází přes příkaz WHOIS,

b) email neinformuje – adresu nepoužívat nebo podrobně zkontrolovat zda souhlasí s adresou obvykle používanou),

- IDN (International Domain Name): v některých doménových jménech se mohou vyskytovat také národní znaky (pro cz by šlo žluťoučkýkůň.cz), při převodu do ASCII se však stane, že dvě různé domény může prohlížeč vyhodnotit jako jednu a tu samou.
obrana: vypnutí IDN (není ideální, ale je účinné), anebo pečlivě kontrolovat cíle odkazů,
- přihlašování se z jiných stránek: nabídnutí přihlášení se k jisté službě z jiné stránky (autor „prokazuje“ službu usnadněním přihlášení), toto přesměrování může opravdu fungovat a člověka k dané službě přihlásí, ale zároveň může dojít k uložení údajů někam do databáze a následnému zneužití.
obrana: těmto „pomocným“ stránkám se vyhnout,
- chyby, exploity: využívá chyb ve zpracovávání adres (tzv. address nebo status bar spoofingy - objevují se tam jiné adresy, než na jaké člověk skutečně kliká myší), vložení jiných adres do špatně napsaných skriptů, „vyskakujících“ pop-up oken atd..
obrana: sledování bezpečnostních serverů informujících o známých chybách prohlížečů, aktualizace. [I-13]

Poznámky na závěr:
1) Jen pár čísel - v září 2003 vydala Federal Trade Commission zprávu, že obětí krádeže identity se díky podobným podvodům za uplynulý rok stalo 9,9 milionu obyvatel USA, přičemž náklady firem a finančních institucí s tím spojených dosáhly 48 miliard dolarů a zákazníci přišli o 5 miliard dolarů.

2) Naší zemi se problematika phishingu zatím poměrně úspěšně vyhýbá. Ještě že většina těchto podvodným emailů je v angličtině a stránky napodobují firmy nám neznámé nebo služby nám zatím nedostupné. V budoucnu s růstem internetových přípojek a počtem služeb se ale dá něco podobného dozajista očekávat i u nás.

3) Hlavní je nebýt přehnaně důvěřivý. Solidní firmy a instituce by se nikdy neptaly prostřednictvím emailu na opravdu citlivé informace. V případě obdržení podobného emailu je vhodné do firmy zavolat a ujistit se, zda se jedná opravdu o její požadavek, případně ji rovnou upozornit na existující nebezpečí.

4) Phishing je v současné době považován za formu trojského koně a nové antiviry jej odstraní již automaticky.

5) Několik ukázek phishingu jsem vložil do příloh (příloha číslo 6).

3.4.2 Pharming

Pharming je v podstatě velice blízký phishingu - jedná se o mladší, sofistikovanější a nenápadnější způsob na okradení uživatele o citlivé údaje. Název této metody je zkomolenina anglického farming, což znamená zemědělství či hospodářství. Princip pharmingu je totiž takový, že dochází k „překopání“ dat v počítači oběti.

Nejslabším místem phishingu je jeho podvržená webová stránka, určená ke sběru (krádežím) dat. Jméno této stránky musí vypadat důvěryhodně a podobně - takovéto odchylky si však uživatel může všimnout (anebo tuto falešnou adresu vůbec nepoužije a na stránku přejde přes oblíbené položky) a pak hned pochopit, že se stal obětí podvodu.

Pharming právě toto nejslabší místo eliminuje. Ke své činnosti využívá překladu jména serveru na odpovídající IP adresu, útočí tedy na DNS (využívá k tomu technologie označované jako „DNS cache poisoning“ - „otrávení paměti záznamů DNS“). Potom, když uživatel ve svém prohlížeči zadá adresu například http://ebanka.cz/, nedojde k přeložení IP na správnou 212.67.66.162, ale na nějakou jinou a dojde k přesměrování na podvrženou webovou stránku (která na první pohled vypadá naprosto stejně jako originální). Nic netušící uživatel tedy zadá požadované přihlašovací údaje a neštěstí je hotovo.

Útočníci si pro své útoky snaží najít nějaký špatně zabezpečený DNS server / uživatelovo PC. Při úspěšném útoku na DNS server se pak nic netušícími oběťmi stanou všichni, kdo se chtějí na daný web dostat. Pharming tak dovádí phishing k mnohem větší účinnosti a navíc jeho prostřednictvím může být poškozeno mnohem více uživatelů najedou. Najít slabinu v zabezpečení DNS serveru ale naštěstí není nic snadného.

Napadnutí uživatelova PC je mnohem jednodušší, tam se dá očekávat o dost menší míra zabezpečení. Po úspěšném napadnutí PC (například použitím podstrčeného trojského koně) pak již jen stačí upravit speciální soubor Hosts (C:\windows\system32\driversetc\hosts), který obsahuje URL a jim přiřazené IP adresy.

Ukázka pharmingu pomocí modifikace hosts souboru

1) útočník vytvoří na první pohled identickou kopii stránek (banka.cz), kterou použije k získání údajů,
2) tuto stránky umístí na stroj s IP např. 213.29.7.234,
3) do souboru hosts na vybraném počítači pak přidá řádek: 213.29.7.234 banka.cz,
4) čeká, až se oběť přihlásí ke svému účtu na banka.cz.

Obrana: Proti úpravě IP adresy na napadeném DNS serveru se příliš bránit nedá, ale tento typ útoku je na druhou stranu méně pravděpodobný (lze kontrolovat IP adresy přes příkaz WHOIS).

Proti útoku na počítač je jako ve všech předcházejících případech třeba aktualizovaný a správně nakonfigurovaný firewall a antivirový program, dále aktualizovaný OS. Nikdy také není na škodu dávat si pozor na nedůvěryhodné adresy a pečlivě prověřovat stažené soubory.

Poznámky na závěr:

1) O tom, že tento způsob útoku je nyní na vzestupu, svědčí již zveřejněné případy, kdy útočníci přesměrovali návštěvníky serverů eBay, Google či weather.com na podvržené stránky, kde se jim pokoušeli nainstalovat do počítače spyware.

2) K obraně stojí za vyzkoušení také aplikace Necraft Toolbar (http://toolbar.netcraft.com/), která však zatím funguje bohužel pouze v prohlížeči IE. Při jejím použití se u každé zobrazované stránky vypíší doplňující informace - např. země, do které navštívená adresa náleží, nebo hodnocení jiných uživatelů. S Netcraft Toolbarem se zvyšují šance na odhalení snah o phishing a pharming, případně rovnou lze nějaký nově odhalený podvodnický server udat.

3.5 Sociotechnika

Definice:

„Sociotechnika je ovlivňování a přesvědčování lidí s cílem oklamat je tak, aby uvěřili, že sociotechnik je osoba s totožností, kterou předstírá a kterou si vytvořil pro potřeby manipulace. Díky tomu je sociotechnik schopný využít lidi, se kterými hovoří, případně dodatečné technologické prostředky, aby získal hledané informace.“ [11]

Informační systém je tak bezpečný, jako jeho nejslabší článek. Literatura se shoduje, že tímto nejslabším článkem je takřka vždy člověk (někdy také přezdívaný jako wetvare). Proč by se tedy měl hacker obtěžovat s lámáním technických bezpečnostních opatření, když se tyto údaje může mnohem snadněji dozvědět pomocí sociotechniky?

Sociální inženýr (sociotechnik)

Pod pojmem sociálního inženýra si představíme člověka s různou úrovní počítačové gramotnosti (spíše nadprůměr), který je ale mistrným psychologem a hercem a dokáže získat přístup do systému přes ošálení jeho obsluhy tím, že předstírá, že je osoba s totožností, kterou si pro potřeby manipulace vytvořil (k získaní důvěryhodnosti kromě hereckých schopností ještě využívá například podvržené emaily, SMS, atd.). Díky tomu je sociotechnik schopný využít lidí, se kterými hovoří, případně dodatečné technologické prostředky, aby získal hledané informace.

Zjednodušeně by se tak sociální inženýrství dalo nazvat metodou, která umožňuje získávat informace, přístupy nebo hesla cestou nejmenšího odporu – namísto pracného hledání a zkoušení si o ně sociotechnik jednoduše řekne.

Mediálně nejznámějším sociálním inženýrem je asi Kevin Mitnick, který svého času pomocí svých schopností získal přístup do mnoha amerických systémů. Nakonec byl ale chycen a uvězněn (jeho příběh byl zfilmován, vyšel i knižně), byl mu na několik let zakázán přístup k jakémukoli počítači, ve vězení si odseděl několik let. Po propuštění napsal o sociálním inženýrství knihu [11] a založil bezpečnostní konzultantskou firmu Mitnick Security Consulting.

Obrana proti tomuto typu útoku je velice problematická. Jistého snížení rizika lze dosáhnout přes striktně navrženou a dodržovanou režimovou bezpečnost. Je ale velice pravděpodobné, že sociální inženýři dokáží přijít s metodou, se kterou nepočítáme. Základní obranou je tedy „zdravý rozum“ a vždy mít na paměti, že takovéto riziko existuje a že je permanentně přítomno.

Poznámka na závěr:

1) V případě zájmu o sociotechniku doporučuji [11]. Velice zajímavý je také článek z časopisu [10] s názvem „Hrozí Vám sociotechnický útok?“ (září 2004), kde jsou představeny základní metody, které sociální inženýři ke svým podvodům používají. Přičemž každé zvýšení povědomí o těchto útocích se jednou může projevit jako neocenitelné.

3.6 Další bezpečnostní hrozby

3.6.1 Instant Messaging

Komunikace přes IM programy se těší čím dál tím větší oblibě, a to nejenom v nekomerční sféře, tato forma komunikace dorazila i do mnoha větších či menších firem, kde IM programy slouží jak pro komunikaci s klienty (hlavně podpora, rady, nápovědy), tak pro vnitropodnikové dorozumívání. IM programy v sobě kromě výhod emailů přinášejí i řadu nových – ještě větší rychlost komunikace a lepší souvislost, kompletní historii, informace o statusu druhé strany atd.. Popularitu tohoto typu spojení asi nejlépe prokazuje odhadovaný počet uživatelů, který v současnosti dosahuje 300 milionů. Do konce roku 2006 by množství zpráv vyměněných skrze IM dokonce mělo překročit počet zaslaných emailů.

Většina těchto klientů poskytuje možnost spojení v nejrůznějších podmínkách tím, že nabízí různá nastavení připojení do sítě. Díky tomu IM programy umožňují komunikaci i přes firewally, proxy servery a jiné „omezující“ prvky.

Druhou stranou věci je to, že s tím také přinášejí možnost zneužití tohoto nechráněného kanálu - například přenos škodlivého SW přes standardní přenosové funkce IM klienta, spuštění škodlivého SW přes chybu kódu IM klienta, odposlechnutí probíhající komunikace apod..

Očekávat lze také vzrůstající množství spamových zpráv, někdy také doprovázených zavádějícími odkazy vedoucími na stránky s potenciálně škodlivým obsahem. Tyto zprávy jsou přitom o něco nebezpečnější než podobné typy zpráv z emailu, protože jejich sofistikovanější verze dokáží podle vyplněných profilů tuto zprávu doručit v příjemcově jazyce, čímž zpráva získá na důvěryhodnosti. Občas také po IM sítích kolují poplašné zprávy šířené samotnými uživateli - takzvané HOAXy (viz. podkapitola 3.3.1 Hoax).

Při šíření počítačových červů přes IM je alarmující hlavně rychlost, s kterou se dokáží po těchto sítích šířit. Doba potřebná pro nakažení 500.000 počítačů je v případě IM červů asi 30-40 sekund, u červů šířících se přes emaily je to 20 minut, u červů šířících se po TCP/IP je to 14 hodin.

Obranou IM proti škodlivému software, spamu a odposlechu je použití bezpečnějších klientů (originální ICQ není nejvhodnějším IM klientem pro síť ICQ apod., dobré pověsti se těší Miranda či Trillian), správné nastavení těchto klientů, instalování aktualizovaných verzí, nenásledování podezřelých odkazů, využití zabezpečených komunikačních protokolů pro lokální komunikace (Jabber) s vlastním serverem, využití pluginů jinak zabezpečujících nezabezpečené protokoly (šifrovaní zpráv), doinstalování pluginů pro blokování nevyžádaných správ / s databází zakázaných adres apod..

Pro další informace doporučuji navštívit webové stránky společnosti IMlogic [I-15], která se na bezpečnost IM komunikace přímo zaměřuje.

3.6.2 Jenom krátce o P2P

Peer-to-Peer sítě (zkr. P2P sítě) je označení pro celosvětové distribuované systémy, ve kterých může každý uzel sloužit zároveň jako klient i jako server. Tyto sítě slouží ke sdílení velkého objemu dat mezi uživateli (bohužel většinou zneužívané pro sdílení souborů s nelegálním obsahem). Podle mého názoru sítě P2P jsou velice užitečné pro šíření legálního obsahu, ke kterému by se jinak člověk v našich končinách nedostal. Většinu uživatelů tam ale táhne právě touha po obsahu nelegálním.

Pokud ale uživatel není zběhlý v používání těchto aplikací a správných klientů pro danou síť, nemá ani ponětí o tom, co je „scéna“ a spolehlivý zdroj, tak jen krátce řeknu, že by si to měl s používáním těchto programů dvakrát rozmyslet.

Pro firmy existuje jen jednoznačné doporučení - všechny tyto aplikace zakázat (lze celkem úspěšně přes firewally) a porušení tohoto pravidla tvrdě trestat. Používání P2P *sítí* značně zatěžuje linku (kterou je uživatel / firma připojen-a do Internetu), napomáhá šíření zpravidla nelegálních souborů, vytváří nová bezpečnostní rizika (někteří klienti jsou plní spyware, chyby v klientech umožňují bezpečnostní průniky atd.). V případě, že firma používá linku s limitem přenesených dat, tak tyto sítě navíc zvyšují i náklady na připojení.

Pro zájemce o další informace ohledně bezpečnosti P2P sítí doporučuji dvoudílný seriál článků vycházející v časopise DSM (**Beránek, Ladislav:** P2P systémy a jejich bezpečnost, DSM 2004/6,2005/1, Praha). Pro seznámení s technologií P2P zase stránky http://www.sdileni.cz.

3.6.3 Wi-Fi

O tom, že většina uživatelů bezdrátových technologií takřka doslova ignoruje rizika spojená se zpřístupněním své sítě komukoli v dosahu signálu, už bylo napsáno mnoho (viz. například z nedávné doby: [I-05], 12. 10. 2005., Bezpečnost Wi-Fi sítí v Praze je zatím tragická – zpracováno na podkladech Wireless Security Survey 2005, kterou prováděla společnost Ernst & Young).

Bezdrátové sítě vysílají veřejně SSID, často bez jakéhokoli zabezpečení (např. filtrování MAC adres) nebo pouze se zapnutým WEP šifrováním.

Neoprávněný uživatel pak může ze svého přístroje získat nejen neplacené připojení k internetu, ale u velmi špatně zabezpečených sítí též přístup k datům na sdílených discích pracovních stanic či serverů. Případná škoda se pak nemusí týkat jen neoprávněného získání a zneužití dat, ale též jejich smazání.

Doporučené kroky pro zvýšení bezpečnosti Wi-Fi sítí jsou:

1) omezit její dosah pouze na areál budovy: nepoužívat zbytečně silné antény, zvážit použití směrových či panelových místo všesměrových, vlastnit AP s možností regulace výkonu apod.,

2) skrytí identifikátoru sítě - SSID: pokud není síť určena pro veřejné použití, je vhodné vysílání identifikátoru vypnout, dále přednastavit původní SSID na náhodnou kombinaci písmen, čísel a symbolů (pravidla stejná jak u tvorby hesla),

3) nespoléhat na WEP: lze odposlechnout, dekódovat, zpomaluje provoz (hlavně 128bit klíč), problémy s kompatibilitou mezi kartami, při volbě nového klíče je nutné nastavit jej správně na všech zařízeních – komplikuje správu větších bezdrátových sítí, lepší je umožnit přihlášení k AP všem a bezpečnost řešit až na další úrovni (např. VPN), tento druh zabezpečení je dostatečný pro domácí použití, k odstínění náhodných pokusů o vniknutí do sítě,

4) filtrování MAC adres: omezit přístup pouze pro povolené hardwarové adresy, nutné zanést do seznamu AP, lze odposlechnout povolenou MAC adresu a tu následně zneužít,

5) použít WPA: novější technologie šifrování než WEP, silnější šifrování, přístup do sítě hlídán přes sofistikovanější protokoly než WEP, místo statických klíčů používá technologii klíčů TKIP (Temporal Key Integrity Protocol), klíč je zašifrován hash funkcí, je hlídána jeho integrita, problém je nekompatibilita se staršími Wi-Fi zařízeními,

6) firewall k odstínění Wi-Fi sítě od vlastní firemní sítě,

7) nasazení VPN.

4. Možnosti snižování bezpečnostních rizik IS/IT

V této kapitole bych rád představil vybrané mechanismy, pomocí nichž lze dosáhnout snížení rizika výskytu bezpečnostních incidentů / dopadu těchto incidentů. Tyto mechanismy jsou v dnešní době vitální součástí zabezpečeného IS zajišťující jeho dostupnost. Stejně tak pomáhají zajistit důvěrnost a integritu jeho dat.

Bezpečnostní mechanismy se dají rozdělit na tři hlavní skupiny: preventivní (odstraňují zranitelná místa - antivirové a antispamové programy, firewally, apod.), heuristické (snižují riziko ohrožení), detekční a opravné (minimalizují účinek útoku - např. zálohování).

Většina dnes užívaných obraných mechanismů je rázu technického, organizace stále podceňují kvalitní školení zaměstnanců k zodpovědnějšímu přístupu k otázce bezpečnosti a odpovědnost za udržení bezpečného IS tak leží na bedrech pracovníků bezpečnostních oddělení / správců IS.

Také bych rád zmínil dle mého názoru velice zajímavý druh software určený k „nalákání“ a studování útočníků.

4.1 Antivirové programy

Antiviry jsou programy zaměřené na ochranu počítače před škodlivým SW. Tuto funkci vykonávají přes rezidentní ochranu hlídající veškeré spouštěné programy a známá nebezpečí šířící se po nezabezpečených sítích, moduly pro kontrolu pošty, automatickou / na vyžádání kontrolou výměnných médií / souborů / adresářů / disků, speciálními moduly na dokumenty MS Office atd. (tyto moduly podle svého zaměření pátrají po napadených souborech, v případě nalezení takového souboru má uživatel možnost tento soubor smazat, odeslat do karantény, na výzkum k tvůrci antivirového řešení, pokusit se o jeho „vyléčení“).

V dnešní době jsou komplexní antivirová řešení nezbytnou nutností pro udržení chodu IS organizace. Je vhodné je instalovat jak na klientské počítače (ochrana před uživateli samými), tak v kombinaci s firewallem na vstupní bránu do internetu před pronikáním hrozeb z venku.

Nutnou podmínkou pro zajištění maximálně možné ochrany je pravidelná aktualizace - nové hrozby se objevují takřka dennodenně (některé antiviry obsahují i informátor o nových celosvětových hrozbách (Outbreak Alert), kterým výrobce antiviru nabádá ke zvýšení opatrnosti při pohybu po Internetu) a v první fázi jsou nejnebezpečnější. Rychlost vydávání aktualizací již závisí na samotném výrobci antivirového SW. Může se jednat o hodiny, dny, týden atd.. Důležitá ale není samotná periodicita vydávání aktualizací, ale rychlost reakce při zjištění nové hrozby!

Na trhu existuje velké množství produktů v rozličných variantách (základní balík, rozšíření, pro jedno PC, serverová verze, atd.). Pro výběr vhodného řešení je třeba vzít v úvahu rychlost / kvalitu (počet identifikovaných vzorků z celkového počtu předložených virů on-demand, on-access, počty falešných poplachů atd.) skenovacího procesu, podporu síťové správy, kvality plánovače testů, rychlost vydávávání aktualizací, požadavky na systémové prostředky, podpora více jazyků, počet dalších rozšiřitelných modulů, přehlednost atd..

Na Internetu lze také nalézt srovnávací testy jednotlivých antivirových řešení, patrně nejuznávanějšími jsou ty na stránkách Virus Bulletinu (http://www.virusbtn.com).

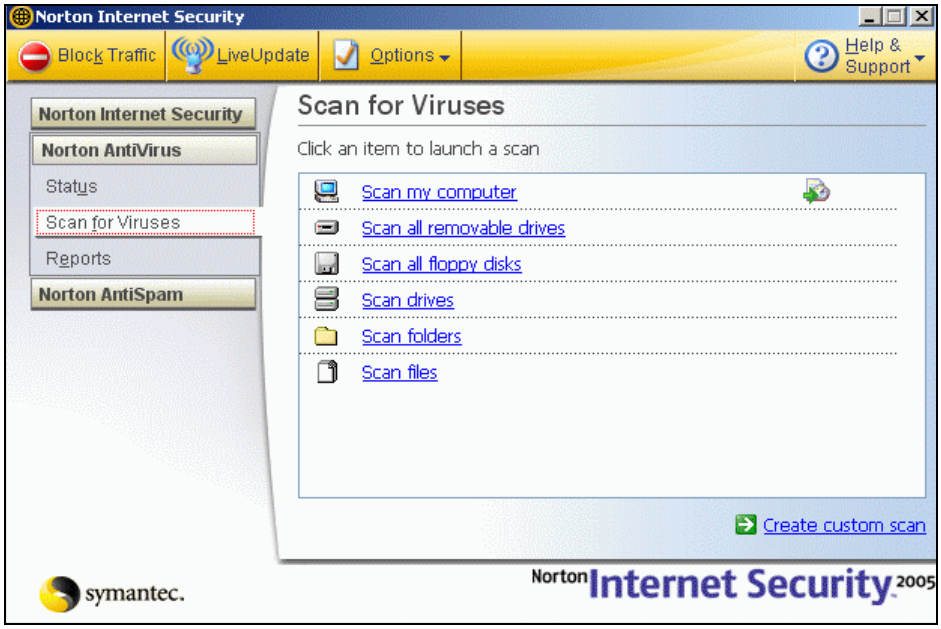
4.1.1 Technologie antivirových programů

Viry lze vyhledávat vícero způsoby. Základním přístupem je vyhledávání na základě **testu signatur.** Tento test je založený na předpokladu, že každý virus obsahuje unikátní řetězec (signaturu), kterým je možné ho jednoznačně identifikovat. Pokud se nějaká taková signatura objeví v testovaném souboru, soubor je napaden daným virem.

Databáze signatur navíc může být doplněna pravidly (co odstranit / pozměnit a jak atd.), které umožňují daný soubor „zachránit“.

Tento druh testu měl v počátku problémy s mutujícími (mění během šíření svojí podobu) viry, v současné době již tuto detekci většina lepších antivirových programů zvládá bez problémů (generická detekce). Výhodou této metody je její rychlost, nevýhodou pak nedetekovaní virů dosud nezanesených ve virové databázi.

Obrázek číslo 4: Norton Internet Security 2005, Antivirus - On-demand nabídka testů



Zdroj: Vlastní tvorba

Druhým způsobem je testování souborů pomocí **heuristické analýzy.** V průběhu analýzy se používají 2 metody. První z nich je heuristická analýza **statická**; ta podrobně zkoumá obsah souborů na pevném disku a vyhledává v nich podezřelé konstrukty (instrukce jako přímý zápis do boot sektoru atd.). Druhou heuristickou metodou je analýza **dynamická**; tato metoda spustí daný soubor v chráněném prostředí virtuálního počítače uvnitř antivirového programu a hledá typické akce, odpovídající chování viru. Příkladem může být program, který vyhledává spustitelné soubory a modifikuje je.

Heuristická analýza je obecně použitelná metoda, nezávislá na virové databázi. Může proto organizaci pomoci i s odchycením dosud neznámého viru, který by jinak mohl způsobit značné škody.

Nevýhodou tohoto typu testování je pochopitelně jeho nižší rychlost. Také přesnost nikdy nebude stoprocentní, tu a tam se objeví planý poplach (u některých antivirových produktů více než tu a tam). Další nevýhodou je neschopnost analýzy daný virus pojmenovat (k tomu je třeba, aby byl vir zanesen v databázi signatur). Ze stejného důvodu nemůže analýza daný soubor vyléčit.

Existují i další metody detekce potencionálního napadení souborů virem. Mezi ně patří například takzvaný **srovnávací test**, kdy po instalaci antivirový program pořídí kontrolní součet (CRC Check) důležitých systémových a dalších potenciálně „virově zajímavých“ souborů**.** Tento kontrolní součet potom pravidelně opakuje a v případě nesrovnalostí upozorní na možný výskyt viru. Tento způsob testování není použitelný na soubory, u nichž se často mění velikost. Nevýhodou je znovu výskyt planých poplachů (systémové soubory se někdy mění přirozeně), neschopnost pojmenovat virus, neschopnost daný soubor léčit.

Poznámky na závěr:

1) Díky rostoucímu počtu bezpečnostních incidentů a jejich medializaci se z vývoje antivirových řešení stává docela dobrý business. (Výňatek z článku „Výrobcům antivirů červi prospívají, přinášejí jim rekordní zisky“, [I-04], 02 2004: „V uplynulém čtvrtletí rostl meziročně zisk největšího výrobce antivirových programů firmy Symantec o 55 procent na 111,5 miliónu dolarů. Konkurenční Network Associates se z loňské čtvrtletní ztráty 11,2 miliónu dostala do zisku 41,3 miliónu. Světová trojka Trend Micro zvýšil zisk o 57 procent na 34,2 miliónu dolarů.“)

2) Existují i teorie, že v případě „virového sucha“ si autoři antivirových řešení nějaký ten virus sami naprogramují.

3) Při rozsáhlých epidemiích antivirové společnosti zdarma vydávají takzvané jednoúčelové antiviry určené k detekci a odstranění této nákazy – neocenitelná pomoc v případě, že systém je napaden.

4) Pro uživatele PC nemající nainstalovaný žádný antivirový program existuje možnost kontroly zdraví počítače online (například http://housecall.trendmicro.com/, http://www.kaspersky.com/).
5) Zájemcům o tuto problematiku doporučuji navštívit české stránky na http://viry.cz. Přehlednou formou zde naleznou mnoho zajímavých sekcí, přehledy antivirů, recenze, aktuální informace a spoustu dalších zajímavých odkazů.

4.2 Firewally

Firewally jsou v podstatě omezovače síťového provozu a jejich hlavní funkcí je ochrana proti útokům zvenčí. Tento útok může být veden odkudkoli a jakýmkoli způsobem. Základním pravidlem tedy je povolit jen nezbytné minimum činnosti v komunikaci mezi firewallem / světem (snížit počet „vstupních bodů"). Implicitně tedy vše zakážeme a pak již jen pomocí pravidel povolujeme to, co je nezbytně nutné (pravidla mají podobu vybraná aplikace, připojení ven, dovnitř, oběma směry, na určitý / jakýkoliv počítač, seznam portů, časové okno, atd..).

Prvním krokem k dosažení bezpečnosti je být schopen ohlídat veškerá spojení ven / do organizace – tedy centralizovat propojení s vnějším světem (přes bránu). A právě na tento centrální přípojný bod je vhodné nainstalovat a správně nakonfigurovat firewall. (v případě, kdy by každý PC měl vlastní přístup na Internet, by se situace stala značně nepřehlednou).

Firewall je povahy SW (program běžící na vyhrazeném počítači), HW (sofistikované zařízení zapojené mezi chráněnou sítí a vnějším světem, často doplněné o aktivní síťové prvky) a jeho úkolem je propojit sítě s různou důvěryhodností tak, že sníží (předem definovaná) rizika vyplývající pro chráněné sítě z tohoto propojení.

4.2.1 Technologie firewallů

Technologie používané při tvorbě firewallů lze rozdělit do několika skupin, přičemž reálný firewall kombinuje několik popsaných technik. Základní technologie jsou: **jednoduchý IP filtr, stavový IP filtr, proxy.**

Jednoduchý a stavový IP filtr

Jednoduchý IP filtr funguje pouze jako blokovač internetového provozu. Podle předem dané sady základních pravidel zakazuje provoz na vybraných portech. Co není zakázáno, je povoleno (pracné nastavování). IP filtr je opravdu jen velice jednoduché zařízení, nemůže analyzovat procházející data a povolovat či zakazovat jejich průchod podle významu. Pomocí

tohoto zařízení lze velice snadno omezit možnost zaměstnanců v jejích přístupu do internetu (zákaz vybraných webových stránek, portů pro vybrané služby atd.).

Stavový filtr má v sobě již drobná vylepšení. Pomocí zabudované „tabulky stavů“ a monitorování síťového provozu je schopen přes změny v této tabulce a předem daných pravidel lépe ohlídat probíhající komunikace. V tabulce stavů si totiž zaznamenává právě spuštěné aplikace z firemní sítě, které se snaží komunikovat se světem venku (přes protokoly vyšší vrstvy - TCP,UDP). Povolí jakýkoli průchod ven, dovnitř ale pustí jen pakety z této zevnitř vyvolané komunikace. Díky tomu má alespoň nějakou možnost kontroly podle aplikační vrstvy.

Proxy

Aplikační proxy je nejpokročilejší metodou pro tvorbu firewallů. Jedná se o program určený pro jeden konkrétní protokol, který filtruje pakety podle toho, která aplikace a na kterém portu s nimi pracuje (port 21 pro FTP přenosy, pouze pro FTP klienty, ostatní programy k tomuto portu nemají přístup). Klientský program pro danou službu nekomunikuje přímo se serverem na Internetu, ale pouze s místní proxy bránou na firewallu. Ta prověří, zda jednotlivé požadavky klienta jsou korektní, a jednotlivé příkazy posílá skutečnému serveru na internetu. Klientské aplikace tak nikdy přímo nekomunikují se servery, ale pouze s jednotlivým aplikačním proxy pro jednotlivé protokoly. Proxy brány obvykle neposílají do Internetu přímo IP adresy klientů lokální sítě, ale překládají všechny lokální adresy v odcházejících paketech na jedinou „venkovní“ adresu. Při příchodu odpovědí je tato „venkovní“ adresa vyměněna za adresu lokálního počítače, který službu požadoval. Toto řešení je bezpečnější – celá síť pak z hlediska Internetu působí jako jediný počítač, což výrazně snižuje možnost průniku do lokální sítě zvenčí (tento princip zakrývání IP adres počítačů z vnitřní sítě se nazývá dynamický překlad IP adres).

U starších proxy serverů bylo nutné před zahájením spojení sdělit bráně, s kým a pomocí jakého protokolu chce uživatelův program komunikovat. Moderní proxy brány jsou již uživatelsky mnohem příjemnější, uživatel o existenci takové brány nemusí vůbec vědět. Kvalitní brány také slouží pro filtraci více protokolů současně.

Filtrovány jsou všechny pakety, jejichž propuštění není explicitně povoleno (co není povoleno, je zakázáno), což je zásadní rozdíl oproti IP filtrům – přináší to celou řadu výhod, především rychlejší konfiguraci a vyšší úroveň bezpečnosti. Nevýhodou je, že takováto brána je hůře přizpůsobivá novým protokolům.

Základem každého moderního firewallu je kombinace paketového filtru a aplikačních bran.

Demilitarizovaná zóna

Oblast nechráněná tak dobře jako ostatní části sítě. V ní bývají většinou umístěny servery (webové, poštovní atd.). Nechráněná není doslova. S okolím je propojena firewallem, který dovnitř propouští jen tu komunikaci, která je určena serverům v demilitarizované zóně (např. 80, 110 a 25 pro http, pop3, smtp). Jakékoli jiné snažení o navázání spojení bude odmítnuto.

Zbytek vnitřní sítě je s vnějškem propojen normálním firewallem, který už nyní nemusí propouštět ty porty vyhrazené pro služby, které poskytují servery v demilitarizované zóně. Výsledkem je tedy ještě větší zabezpečení zbytku sítě.

Propojení vnitřní sítě s touto demilitarizovanou zónou lze řešit dvěma způsoby. Buď obyčejným směrovačem bez zabezpečení, anebo jednoduchým firewallem. Doporučoval bych spíše druhou možnost, tímto jednoduchým firewallem totiž odstíníme i potenciální útočníky ze sítě vnitřní.

Umístění firewallu

Běžný firewall umísťujeme mezi dvě sítě, k jejichž uživatelům máme různou důvěru. Většinou tyto dvě skupiny tvoří firma a její síť X zbytek světa, případně vnitrofiremní síť X demilitarizovaná zóna a demilitarizovaná zóna X Internet. Pokud má takový firewall povahu hardwarového zařízení, nebo je jeho běhu dedikován PC, je jeho umístění zcela jasné.

Velice často ale firewall spolu s jinými servery běží na jednom společném počítači. Pak tento firewall plní funkci osobního (chrání ostatní servery na stejném PC, při správné konfiguraci dokonce lze vytvořit i demilitarizovaná zóna). Tentýž firewall může podle jiných pravidel chránit komunikaci mezi vnitřní a demilitarizovanou zónou (o tom jaká pravidla použít rozhoduje analýza záhlaví IP datagramu).

Umístění osobního firewallu je vhodné na každou klientskou stanici (více viz. 4.2.2 Osobní firewally)

Single Point of Failure (SPoF)

Zapojení popsané výše má přes řadu nesporných výhod i jeden obrovský nedostatek, a tím je právě SPoF. Toto schéma totiž vytvoří jeden jediný přístupový bod, při jehož selhání dojde ke kompletnímu odříznutí organizace od zbytku světa. V řadě organizací tento výpadek nepředstavuje nijak zásadní problém nutný preventivního protiopatření (vynaložení prostředků na něj). Existují ale také firmy (služby / aplikace), které si takovéto výpadky dovolit nemohou.

Řešení je technicky poměrně prosté - zdvojíme tyto přístupové body (2x server, 2x firewall, 2x antivir atd.), oba připojíme na hranici a nastavíme tak, aby se o kontrolu síťového

provozu podělily (Load Balancing). Pokud jeden z těchto serverů přestane fungovat, druhý převezme celý provoz kompletně na sebe (failover) a zašle upozornění správci IS.

Toto řešení ale přináší i další výhody. Může sloužit k rozdělení zátěže ve špičkách, kdy zátěž pro jeden firewall by byla příliš veliká. Bez obav lze také na jednom ze zařízení provádět údržbu (restarty, reinstally atd.), celková spolehlivost připojení se díky druhému serveru značně zvyšuje (dalším krokem pro zvýšení dostupnosti může být příprava záložního zdroje energie pro případ výpadků atd.).

4.2.2 Osobní firewally

Ne každá organizace má dost peněz na zakoupení HW zařízení nebo vyčlenění jednoho PC na funkci firewallu. Tam, kde schází prostředky nebo chuť do pořízení nějakého sofistikovaného řešení, pomůže k lepšímu zabezpečení jeden z mnoha existujících osobních firewallů. Osobní firewall je aplikace, která se instaluje do operačního systému PC a která se stará o jeho bezpečnost při přístupu na síť. A není chybou ani plýtváním finančními prostředky vybavit klientské stanice firewally osobními i v případě existujícího firewallu podnikového - klientské počítače se občas ocitnou mimo síť (notebook na cesty a připojení přes modem, Wi-Fi a osobní firewall stále bude chránit PC), ochrání klientská PC před uživateli samotnými, nabízí další uživatelsky zajímavé funkce a dvojitá obrana nikdy není na škodu.

Navíc díky skutečnosti, že tento firewall má na starosti většinou pouze jeden počítač (ten, kde je nainstalován), může analýze výchozích a příchozích dat věnovat mnohem více strojového času. Dále, tyto osobní firewally lze nakonfigurovat přesně podle požadavků konkrétního uživatele (pouze jediný uživatel má právo přistupovat na FTP, tento port se otevře pouze na jeho osobním firewallu atd.). Možností je mnoho.

Osobní firewally v sobě také sdružují další užitečné funkce, ty už ale závisejí na konkrétním výrobci těchto aplikací (blokování reklam, blokování "vyskakovacích" oken, spamové filtry, hlídání změn systémových komponent, nastavení pravidel pro příchozí emaily, předdefinovaná pravidla pro nejznámější programy, udělat počítač na internetu „neviditelným" apod.).

Bezpečnostní boom v minulých letech také přeje "kombo" řešením – osobní firewall a antivirový program sdružené do jednoho balíku, který zajišťuje bezproblémovou součinnou funkčnost (osobně jsem se setkal s problémy s kompatibilitou vzniklou spojením osobního firewallu a antivirového systému od různých výrobců, které končily „modrou smrtí" a nutností restartu Windows). Mezi asi nejznámější patří Norton Internet Security od firmy Symantec,

Mcaffe a jejich Internet Security Suite, Panda Platinum Internet Security od Panda software a další.

Obrázek číslo 5: Norton Internet Security 2005, Firewall - Nastavení

Zdroj: Vlastní tvorba

Konfigurace osobních firewallů není nijak složitá, ze začátku po instalaci je ale vhodné, aby u počítače seděl kvalifikovaný uživatel. V počátečním nastavení je totiž veškerý síťový provoz zakázán. Při spuštění jakékoliv aplikace, která se pokouší dostat „ven“, vyskočí dialogové okno; většinou pomalované výstražnými barvami nebo obsahující vykřičníky; s žádostí o povolení / zakázání / manuální nastavení konkrétního spojení a postupu do budoucna (pravidlo platí dál, pouze jednou, atd.). Některé firewally pro známé programy umožňují automatické nastavení přístupu podle již zmíněných předem připravených pravidel, jiné je ale třeba nastavit manuálně. A tady bývá u méně zkušených uživatelů kámen úrazu. Buďto si omylem nevědomky zakáží přístup některého svého programu na Internet, nebo naopak vytvoří pěknou „díru“ v bezpečnosti svého počítače. Přitom zpětně najít tato pravidla dá někdy docela zabrat. Zde platí ono oblíbené rčení: „Osobní firewall je výborný sluha, ale zlý pán.“

Kvality osobních firewallů lze porovnat podle testů dostupných na internetu, / z papírových magazínů. Tady bych jenom doporučil - nikdy nedávejte na testy firewallů uveřejněných výrobcem daného firewallu - protože domácí většinou nějakým zázrakem vždy vítězí, přičemž mezi seriózními osobními firewally o něm v reálu takřka neuslyšíte.

Pokud jste k Internetu připojeni přímo, tedy se nenacházíte například za proxy serverem poskytovatele, můžete bezpečnost svého PC a firewallu do jisté míry podrobit zkoušce použitím některých online testů, například: (AuditMyPC.com, Sygate.com, TestMyFirewall.com,

PCFlank.com). Pokud jste za proxy, tak místo vašeho firewallu bude otestován proxy server vašeho poskytovatele.

Nejkvalitnější osobní firewall ale také zároveň neznamená nejlepší pro každého. Některé osobní firewally obsahují opravdu až moc možností v nastavení a pomocných pluginů, z kterých jsou možná nadšeni recenzenti a odborná veřejnost, ale které nikdo jiný patrně nevyužije. Dobré je se tedy před jejich nákupem pořádně na trhu porozhlédnout po řešení, které vám nejlépe vyhovuje.

Navíc většina výrobců osobních firewallů umožňuje zpravidla 30 denní lhůtu na vyzkoušení jejich produktu zdarma - a i po uplynutí této lhůtu vám mnoho z nich bude v omezené míře sloužit nadále, takže spěchat s nákupem se opravdu nevyplácí (také můžete zjistit, že jste si domů pořídili pěkně drahé omalovánky, v kterých ale pořádně nejde nic najít, natož nastavit).

Poznámky na závěr:

1) Stejně jako v případě antivirových programů, i firewally je nutné aktualizovat, aby poskytovaly účinnou obranu před nově vzniknuvšími riziky. Některé firewally si aktualizace hlídají samy (podobně jako MS Windows), u jiných je toto necháno na uživateli.

2) Rozhodně není dobré spoléhat na firewall obsažený v SP2 pro MS Windows XP. Tento firewall propadl takřka ve všech pokročilejších testech. Existuje i mnoho zdarma šiřitelných osobních firewallů, které tento předčí na plné čáře.

3) Rozsáhlý, aktuální a přehledný list osobních firewallů včetně recenzí najdete na http://www.firewallguide.com/software.htm (07.11. 2005).

4.3 Antispamové programy a boj proti spamu

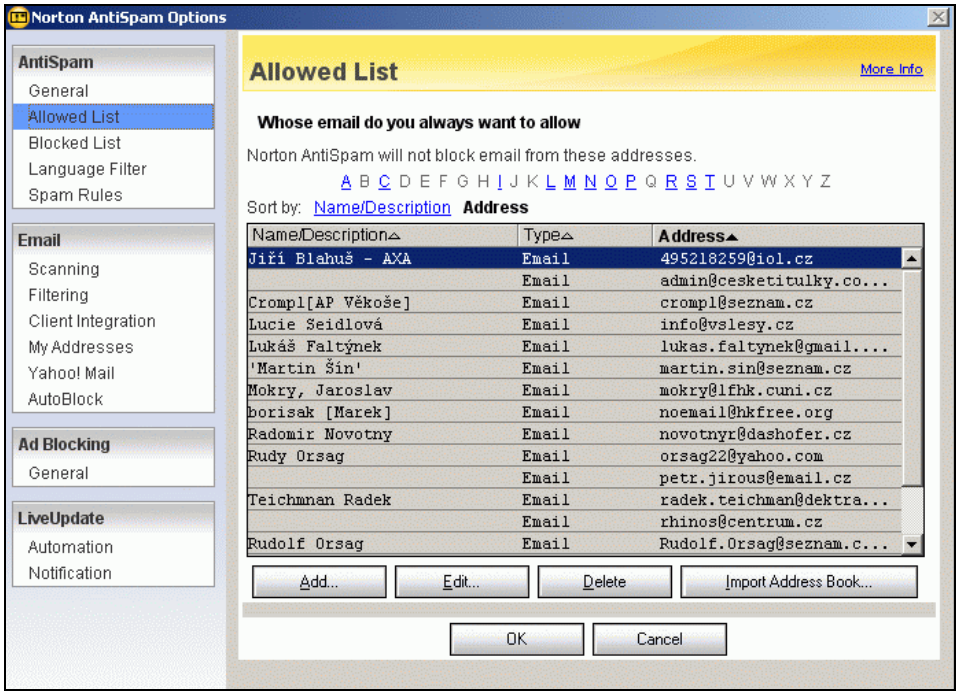
Tyto programy slouží k filtraci záplav nevyžádané pošty - elektronickému „moru“ tohoto století. Antispamové programy jsou většinou součástí větších bezpečnostních softwarových balíků (spolu s antivirovým programem a osobním firewallem), samostatná řešení ale samozřejmě existují také. Umístění je znovu logicky spolu s antivirem a firewallem na vstupní bráně, v případě její neexistence na poštovní server. Se spamem dokáží bojovat vícero způsoby.

Filtrování podle obsahu

Základem je vyhodnocování / filtrování na základě použitých slov obsažených v emailu (porn, Viagra, Cialis atd.). Pokud email překročí určitou hranici, je označen jako SPAM

a odhozen. Tím množství spamu doručené do pošty výrazně klesne. Toto vyhodnocování má ale i své nedostatky; chytře napsané spamy většinou projdou (hodně spamů je na první pohled těžko čitelných, spameři se snaží filtry obejít a tyto citlivá slova přepisují tak, aby vypadala podobně, ale byla složena z jiných znaků, které filtry nezachytí jako např. p0rn, ClALlS, atd.). Na druhou stranu toto vyhodnocování také občas za spam označí a hodí do spamového koše email, na který jste dlouho čekali.

Obrázek číslo 6: Norton Internet Security 2005, Antispam - filtrovaní podle email adres



Zdroj: Vlastní tvorba

Filtrování podle adres

Další metoda spočívá v tom, že při prvním spuštění označíte důvěryhodné adresy, z kterých bude email vždy doručen (whitelist), ostatní emaily budou automaticky zahazovány do spam koše (blacklist), jedná se tedy o filtrování podle adres. Nevýhoda je jasná - budete muset vždy prohlížet spam koš a hledat regulérní neočekávané zprávy - za čas se sice tato databáze důvěryhodných adres rozroste, ve střehu ale budete muset být neustále. Obráceně tato metoda bohužel nefunguje vůbec. Spameři svoje adresy generují náhodně, nebo přebírají databáze existujících lidí, málokdy se stane, že by došlo více spamů z jedné adresy.

Zautomatizování a zjednodušení tohoto procesu mohou přinést tzv. challenge-response metody. Tyto metody pracují tak, že na začátku jsou všechny adresy zakázané. Po přijetí dopisu je systémem automaticky vygenerován zpětný email, ve kterém se po odesílateli žádá potvrzení původního dopisu. Po potvrzení je tato adresa přijata jako validní a je přeřazena ze zakázaných

adres do seznamu adres povolených. Tato metoda má jednu nevýhodu - sekundární obtěžování nezúčastněných třetích stran v případě, že spammer pro svou práci zneužívá něčí reálnou adresu.

Předchozí metody boje se spamem lze chápat jako **metody pasivní**, kdy se snažíte omezit již došlé množství doručených spamů. **Aktivní metoda** boje proti spamu spočívá v něčem trošku jiném, a to ve snížení počtu spamů odesílaných na určitou adresu. V mnoha spamových emailech je totiž na konci nabídnuta možnost odepsat se ze spamového seznamu. Odhlášení je většinou úspěšné, „slušný“ spamer Vás vyhodí z databáze a množství spamu se sníží. Bohužel mnohdy má tato metoda i úplně opačný výsledek, množství spamu v poště ještě vzroste, protože automatický zasílač spamu tímto „odhlášením“ získal další potvrzenou platnou adresu.

Poznámka na závěr:

Pro běžného uživatele je nejlepší obranou proti spamu využívaní více emailových účtů. Ten určený pro opravdu soukromou korespondenci nesmí být nikde zveřejněn (na žádných www, přihlašování k odběru novinek ze zpravodajských serverů, SW produktů, atd., nikdo kromě vašich známých by o něm neměl vědět). Automatičtí spamboti totiž cíleně prohledávají www stránky, databáze a hledají znak „@“ (pokud už potřebujete někde tento email zveřejnit, tak ve zkomolené podobě, nebo jako obrázek - člověk si správnou adresu odvodí, spambot ne). Tím se dá množství spamu pro soukromou korespondenci (a jistou aplikaci má toto řešení i v případě firemních emailů) snížit na minimální možnou úroveň.

4.4 Šifrování a kódování

Metody šifrování a kódování poskytují základní ochranu **utajení dat** ve všech formách jejich elektronické existence (během přenosu, uložení, uskladnění), **autentizaci** – potvrzení o totožnosti subjektu nebo objektu a **integritu informací** (potvrzení o správnosti obsahu přenesené zprávy).

Šifrování znamená proces, kdy z normálních dat (otevřený text) vytvoříme pomocí šifrovacího algoritmu a šifrovacího klíče data šifrovaná – pozměněná (kódovaný text). Přičemž bez znalosti tohoto klíče nelze tyto data převést zpět do původního obsahu.

Kódovací algoritmus má stejnou funkci, do procesu ale nevstupuje žádný klíč, kdokoli se stejným algoritmem může data dostat nazpět.

Existuje mnoho šifrovacích algoritmů, s růstem výpočetního výkonu staré zanikají (nedostatečný počet kroků, krátká bitová délka klíče atd.) a vznikají nové, složitější, schopné

tomuto nárůstu výkonu na nějaký čas odolat. Základní dělení šifrovacích algoritmů je na algoritmy **symetrické** (substituční a transpoziční šifry, stejný klíč se užívá pro šifrování a dešifrování, - problém s bezpečným přenosem klíče, složitá správa klíčů při vícesměrné komunikaci) a **asymetrické** (dva klíče, jeden volně přístupný pro zašifrování zprávy - veřejný klíč, a druhý pro její rozšifrování - soukromý klíč, + jednodušší správa klíčů, - výpočetně náročnější)**.** Mezi nejznámější symetrické algoritmy patří šifra DES (Data Encryption Standard), AES (Advanced Encryption Standard) RC2 a RC4 (Rivest Cipher 2 a 4), IDEA (International Data Encryption Algorithm), mezí asymetrické RSA (Rivest, Shamir, Aleman - tvůrci). Existují i další dělení šifer, například podle množství dat, která sou šifrována v jednom okamžiku na proudové (po znacích) a blokové (větší bloky textu), atd.

O prolomení šifer se útočník může pokusit mnoha metodami. Nejznámější způsob je zkusmým generováním všech možných klíčů (brute force), dále můžeme luštit text se znalostí mnoha šifrovaných zpráv (odhalení klíče analýzou), nebo budeme mít šifrované zprávy a jejich podobu v otevřeném textu (taktéž hledání klíče analýzou), nátlakem na osobu vlastnící klíč nutný k rozšifrování apod..

Využití šifrování k zabezpečení dat

V dnešní době s rostoucími hrozbami a výpočetním výkonem počítačů se vyplatí využít programů / funkcí vlastního OS na šifrování čehokoli (ať už on-line, off-line, on-demand metodou). Šifrovat se vyplatí veškerá důležitá data na lokálních / síťových discích (lze vybrat celý disk, zvolené adresáře, soubory), výměnných médiích (samozřejmostí je šifrování veškerých záloh / archivací), komunikace na LAN / WAN včetně pošty. Základním pravidlem by měla být co nejmenší závislost zabezpečovací šifrovací politiky na uživatelích jednotlivých stanic. Existují transparentní polo / plno automatická řešení nabízející komplexní ochranu (nabídka například na http://www.aec.cz).

Poznámka na závěr:

S rostoucí oblibou a využíváním notebooků je aktuální otázka zvýšení jejich zabezpečení. Mnoho pracovníků s těmito notebooky jezdí na služební cesty, nosí si je po práci domů. Notebooky může přitom poměrně snadno někdo odcizit, notebook lze ještě snadněji někde zapomenut. Kvalitní šifrování program zajistí, že se útočník / nálezce k ničemu jinému než k notebooku samotnému nedostane (šifruje se vše). Hlavně se nespoléhat pouze na hesla bránící vstupu do počítače. Není nic jednoduššího než heslo prolomit (díky tomu se nedoporučuje využívat ani Windows nativních šifrovacích technologií Encrypted File System, EFS - klíč není

možné umístit na přenosné médium, zůstává chráněn pouze uživatelským heslem), nebo daný disk vyndat a dát do jiného počítače. [10]

4.4.1 Elektronický podpis

Tento druh podpisu lze použít pro podepsání elektronického dokumentu (souboru) libovolné délky a obsahu. Podpis je tvořen řetězcem bajtů, který je připojen k danému dokumentu. Délka řetězce závisí na algoritmu a požadovaném stupni bezpečnosti (druhu certifikátu). El. podpis **zaručuje autenticitu dokumentu** (příjemce dokumentu bezpečně ví, kdo je autorem), **integritu dokumentu** (příjemce má jistotu, že obsah dokumentu nebyl během přenosu modifikován třetí stranou), zajišťuje **nepopiratelnost autora** elektronického podpisu (nemůže popřít autorství dokumentu ani obsah).

Pro el. podpis se nejčastěji používá asymetrická šifra RSA (Rivest, Shamir, Aleman - tvůrci) a DSA (Digital Signature Algorithm). Při vytváření podpisu se nejprve spočte zkrácená charakteristika zprávy (hash přes jednosměrnou hashovací funkci, např. MD5 - Message Digest Algorithm 5, SHS - Secure Hash Standard). Z hashe se pomocí soukromého klíče spočte elektronický podpis, který se ke zprávě připojí.

El. podpis je spojen s jedním konkrétním dokumentem a nemůže být použit k podepsání dokumentu jiného, může být vytvořen pouze osobou oprávněnou (mající soukromý klíč), je nemožné vytvořit jiný dokument, sebeméně odlišný, pro který by byl původní podpis stále platný. Jakmile je elektronický podpis dokumentu vytvořen, kdokoli si může pomocí veřejného klíče prověřit platnost podpisu. Pokud je platnost v pořádku, příjemce má jistotu, že zpráva byla podepsána vlastníkem soukromého klíče a že po podepsání nebyla modifikována. Příjemce navíc může předložit nezávislé třetí straně podepsanou zprávu jako důkaz o tom, že odesílatel tuto zprávu odeslal a odesílatel tuto skutečnost nemůže popřít (dlužné dopisy atd.).

Elektronický podpis lze díky jeho vlastnostem použít v řadě aplikací, jako například elektronická pošta, právní systém (časová razítka), elektronické provádění plateb, obchodní aplikace, distribuce SW, zajištění integrity databáze aj..

Certifikovaný klíč a certifikační autorita

Certifikovaný klíč se používá k zaručení pravosti elektronického podpisu (že opravdu patří k osobě, která ho vydává a není někým podstrčen). Certifikovaný klíč je klíč získaný od důvěryhodné „třetí strany“ (certifikační autorita), která zaručuje pravost elektronického podpisu. Certifikační autorita stvrdí svým podpisem, že konkrétní veřejný klíč patří konkrétní

osobě a tento „potvrzený“ veřejný klíč již není problém přikládat ke každému dokumentu. Příjemce pak nejprve ověří podpis v certifikátu, pokud souhlasí, ověří osobní údaje uvedené o odesílateli v certifikátu. Pokud i tyto údaje souhlasí, může přiloženému veřejnému klíči věřit a použít ho k ověření digitálního podpisu vlastní zprávy. Ještě předtím je třeba ověřit, zda tento certifikát je platný – buď na stránkách certifikační autority (seznam CRL - Certificate Revocation List), nebo se tak děje automaticky (OCSP – Online Certificate Status Protocol), nutné stálé připojení k Internetu).

Certifikát na veřejný klíč může obsahovat takřka libovolné údaje. Existuje ale celá řada norem (ITU X.509 aj.), právních předpisů a úmluv, které tyto údaje mohou přesně vymezit.

Existuje několik tříd certifikátů lišících se mírou ověření identity vlastníka (class 1-4). V naší republice je vyžadován certifikát 3. třídy, kdy žadatel musí osobně navštívit certifikační autoritu, která předepsaným způsobem ověří jeho totožnost.

V České republice je používání eletronického podpisu vymezeno zákonem č. 227/2000 Sb. o elektronickém podpisu a vyhláškou č. 366/2001 Sb. o upřesnění podmínek stanovených v § 6 a 7 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu.

4.5 Zálohování dat

V druhé a třetí kapitole bylo upozorněno na mnoho způsobů, kterými se dá velice snadno přijít o data. Každá taková ztráta dat může dočasně zastavit chod celé organizace a tím ji značně poškodit (finanční, kvalitativní škody). Cílem zálohování je rychle obnovit tuto ztrátu dat a zajistit plně funkční stav IS v podobě, v níž byl těsně před katastrofou. Zálohování je prostředkem pro udržení dostupnosti informací (k nějaké ztrátě právě rozpracovaných dat sice pravděpodobně dojde, záleží na pravidelnosti zálohování, ale stále je to nicotná ztráta v porovnání s případem, kdy by zálohování nebylo prováděno vůbec).

„Dobře zvolená, propracovaná, a zejména dodržovaná strategie ukládání a zálohování dat je naprosto nezbytná pro nepřerušený chod moderní organizace. [I-08]

Ukládání a zálohování dat není na poli IT ničím novým. Páskové technologie a autoladery / knihovny jsem se rozhodl z důvodu rozsahu práce a poměrné „věkovitosti“ vynechat - o těchto technologiích už toho bylo napsáno více než dost, případní zájemci naleznou širokou nabídku těchto produktů na [I-08], navíc díky klesajícím cenám, zvyšujícím se kapacitám a mnohem

rychlejším přístupovým dobám u pevných disků je tato technologie již spíše na ústupu a je nahrazována diskovými poli. Vedle původní otázky „kam s nimi“ se dnes ovšem v souvislosti s novými riziky objevuje otázka nová: „jak ztracená data rychle obnovit“. Cílem je mít data zálohovaná tak, aby se zabránilo ztrátě nebo poničení dat a aby vybraná data byla v případě nutnosti rychle dostupná, v mnoha případech v reálném čase.

Organizace má v případě zálohování svých dat možnost zvolit realizaci buď vlastními silami, nebo může svěřit péči o svá data specializovanému poskytovateli služeb zálohování. Outsourcing s ohledem na zálohování dat v případě katastrof je stále častější i pro menší podniky.

Zálohovat lze na média magnetická, optická, magneto optická, s možností přepisu (USB/HDD, HDD, CD, DVD, FLASH, pásky DAT, DLT, AIT – liší se kapacitou, rychlostí zápisu, cenou, spolehlivostí).

Zálohování X archivace

Proces zálohování se liší od archivace dat. Za archivní data se považují data uložená na bezpečném místě, která jsou uschována pro případ dalšího pozdějšího užití. Životnost archivací se počítá na desítky let. Na archivaci je vhodné použít jiných medií a postupů než pro běžné zálohování.

Způsoby zálohování

Existuje několik základních způsobů zálohování. Prvotní zálohování se nachází **výchozí.** Při něm dojde ke kompletní záloze všeho. Další zálohování jsou buď **kompletní** (zálohuje se vše najednou, nejpoužívanější metoda, + jednoduchost obnovy, - zabírá víc místa a náročnější na systémové zdroje), **inkrementální** (první spuštění kompletní záloha, další zálohy pouze od minule změněná data, po určitém čase / počtu spuštění opakování celého procesu, + časová a objemová nenáročnost, - složitější skládání kompletního obrazu systému v případě obnovy) nebo **diferenční** (obdoba inkrementálního, s každým dalším spuštěním zálohuje VŠECHNY změny od poslední kompletní zálohy, + odpadá potřeba obnovy dat z více záloh, - o něco náročnější na úložný prostor než inkrementální metoda). Každá z výše uvedených metod je vhodná pro jiný typ dat. Data s vysokou frekvencí změn se nevyplatí zálohovat inkrementálně nebo diferenčně, naopak data s měnícím se pouze zlomkem celkového objemu se vyplatí zálohovat inkrementálně a diferenční metoda se hodí pro případy nutnosti rychlé obnovy dat.

Zálohovat můžeme za chodu systému v reálném čase (Hot Backup), při zastavených / běžících procesech IS (Online / Offline Backup), dále může zálohovat naprosto vše bez kontroly

změny dat / zálohovat znovu pouze změněná data (Full / Incremental Backup). Případnému obnovení se v anglické terminologii říká "Restore".

Z pohledu způsobu vytváření záloh lze zálohování rozlišit na centralizované a decentralizované. **Decentralizované** zálohování již patří spíše minulosti, metoda byla založena na individuální péči uživatele o data. Každý uživatel si zálohoval svoji práci dle vlastního uvážení, data nahrával na jiná média (diskety atd.). Často došlo ke ztrátě dat díky nechtěnému přepsání, technické nespolehlivosti nevyspělých médií, opomenutí - z pohledu organizace se jednalo o neefektivní činnost. Tento postup je v dnešní době použitelný jen u jednotlivců / malých firem.

Centralizované zálohování je založeno na využití velkokapacitních ukládacích center, přičemž tyto centra jsou na vysokorychlostních sítích dostupné i z koncových stanic. Centrální zálohování využívá automatickou úschovu dat. Automatika odstraňuje nespolehlivý lidský faktor, plánované akce provádí pravidelně, svojí činnost dokumentuje, hlídá technický stav zálohovacích mechanik, informuje správce IS o výsledku činnosti atd..

Rady pro zvládnutí práce s daty

Znát podniková data a prostředky k jejich ukládání, znát předpisy ohledně uchovávání specifických kategorií dat, zajistit dostatečnou odolnost úložných médií, stanovit politiku správy, ukládání a zálohování dat plně vyhovující dané organizaci a sektoru, kde působí, vyčleněný personál v dostatečném počtu a kvalifikaci, politiku ukládání dat dodržovat a plán obnovy prověřovat. [I-09]

Strategie zálohování dat

Plánování zálohování >> Vlastní zálohování (klasifikace důležitosti dat, stanovení časové periodicity tvorby záloh) >> Zpětná obnova (krizový plán obnovy, vlastní obnovení dat).

Technologie pro zálohování

Dnešní technologie ukládání dat jsou velice spolehlivé, trvanlivé, rychlé, málo náchylné na zničení a úsporné z hlediska spotřeby místa pro archivaci. Především se jedná o optická média a optické sítě, které nabízejí nejen jinak nedosažitelnou kapacitu jak samotného paměťového prostoru (gigabytů až terabytů), tak rychlosti přenosu dat (Gbit/s), ale také spolehlivost (trvanlivé optické paměti a malá bitová chybovost u optických sítí).

DAS - Direct Attached Storage - Tento systém je založen na jednom zálohovacím serveru, obvykle dedikovaném, a ostatních serverech, které se k zálohovacímu procesu tváří jako klienti. K zálohovacímu serveru jsou připojeny jeden nebo více disků. DAS používá buď rozhraní EIDE

(známé také pod označením ATA) nebo Serial ATA, či spolehlivější a dražší SCSI. Velmi časté je u této varianty využití diskového pole dle některé ze specifikací RAID. Výhody této varianty jsou její jednoduchost na instalaci a konfiguraci, kde v podstatě stačí nainstalovat požadované souborové a aplikační agenty pro on-line zálohování databázových / poštovních systémů. Nevýhodou je, že všechny informace směrem z i do úložné jednotky musí procházet serverem, takže může dojít k přetížení serveru.

Obrázek číslo 7: DAS zařízení Nexsan ATAboy, Hitachi Thunder 9500V series, Nexsan SATABoy

Zdroj: [I-08]

Po samostatných úložných jednotkách přišly na trh síťové úložné prostředky **(NAS - Network-Attached Storage) -** specializované servery pro připojení úložných zařízení (nejčastěji páskových jednotek a diskových souborů RAID) k síti. NAS zařízení podporují různé operační systémy a protokoly pro přenos a vyhledávání souborů a jsou optimalizovány pro přístup k souborům. Mezi další výhody NAS zařízení patří nízké náklady a jednoduchost implementace i managementu, spolehlivost; nevýhodou je obtížná rozšiřitelnost. Další nevýhodou je, že zařízení NAS spotřebovává prostředky podnikové sítě a může ji nepříjemně zatěžovat a tím ovlivňovat chod podnikových aplikací - nevhodné pro datově intenzivní prostředí.

Od roku 2000 se trend zálohování dat přesunuje z lokálních sítí na samostatné úložné sítě (SAN - **Storage Area Network**) s vysokou dostupností - k centrálnímu datovému úložišti je připojeno více serverů a přenosy dat probíhají po samostatné síti (SAN), nezávisle na počítačové síti LAN. Na rozdíl od klasické architektury, kdy měl každý informační systém svoje servery a každý z nich své datové nosiče, jsou u SAN všechny datové nosiče nahrazeny společnými externími diskovými poli a knihovnami propojenými vysokorychlostními optickými vlákny. Výhody diskových polí jsou tak najednou přístupné pro všechny servery a aplikace. Sítě SAN výrazně snižují náklady na provoz a údržbu datových prostor, umožňují efektivnější přístup k datům a snadné rozšíření kapacity i počtu připojení. Mezi další výhody patří délky propojovací

kabeláže, Fibre Channel (FC) technologie umožňuje propojení na vzdálenost až 10tky kilometrů společně s vyšším přenosovým pásmem (200 MB/s). S postupně vznikajícími SAN infrastrukturami vznikl nápad zařadit do této infrastruktury také zálohování, které mělo hlavní výhodu v tom, že přenos dat byl výhradně realizován právě přes SAN a tím pádem s nulovým zatížením síťového pásma, které je následně plně k dispozici klientským aplikacím.

Základem této varianty je opět zálohovací server, který může být realizován v podstatě na libovolné platformě. Změna nastává v definici klientů. V tomto případě je klient povýšen na tzv. "SAN Storage Node", který má možnost přímo přistoupit na zálohovací jednotku v knihovním systému. Pokud je spuštěn zálohovací proces, klient účastnící se tohoto procesu si vyžádá přidělení zálohovací mechaniky a následně provádí zálohu přes SAN bez účasti zálohovacího serveru. Po skončení zálohování dojde k uvolnění páskového zařízení a to je dále poskytnuto dalším klientům, kteří provádějí zálohování skrze SAN. Funkcionalita sdílení zálohovacích mechanik mezi servery se nazývá Dynamic Drive Sharing (DDS). Po síti jsou následně posílány tzv. metadata, které vznikají u klienta provádějící zálohování a jedná se v podstatě o údaje o aktuálně zálohovaných souborech. Při následné obnově přistupuje administrátor právě do databází, které jsou vytvářeny zálohovacím serverem z metadat.

SAN jsou složité a drahé především kvůli technologii Fibre Channel, na níž stojí. S masovým rozvojem IP sítí a s rozvojem potřeb pro ukládání dat se začalo pracovat na řešeních, která by šla realizovat prostřednictvím IP (iSCSI), navázat na drahou infrastrukturu Fibre Channel, nebo ji úplně nahradit a celkový systém zlevnit. SAN nejsou nástupcem NAS, ani nenahrazují NAS; tato řešení se mohou vzájemně doplňovat, být vzájemně efektivně propojená.

Při správném nasazení SAN se rapidně sníží doba potřebná k zálohování a obnově kritických dat. Další výhodou je vyloučení LAN (a tedy žádný vliv zálohování na provoz podnikové sítě) z procesu zálohování, snadná správa, vysoká úložná kapacita. Nevýhodou jsou pak vyšší pořizovací náklady.

Základní zásady zálohování a archivace pro běžného uživatele / malou firmu z decentralizovaným přístupem

1) Uchovávat data v jednom adresáři a vytvořit pro ně v tomto adresáři přehlednou strukturu. Nejde pouze o pořádek, pokud jsou data rozházeny po všech možných adresářích roste riziko jejich smazání omylem. Navíc v případě archivace po nějakém čase a se zvyšujícím se množstvím medií s archivovanými daty bez struktury geometricky klesá šance na nalezení hledaného.

2) Frekvence, se kterou by měla být data zálohována, závisí na rychlosti, s jakou jsou prováděny úpravy nebo vytvářeny nové soubory. Pokud se pracuje s mnoha soubory je lepší je zálohovat častěji, např. jednou denně. Optimum pro většinu uživatelů představuje zálohování jednou týdně.
3) V případě, kdy není k dispozici vysokokapacitní jednotka, stačí ukládat pouze data, programy je možno znovu nainstalovat.
4) Vždy se vyplatí zálohovat na výměnné médium. Uložení druhé kopie na harddisk/y zvýší sice bezpečnost proti náhodnému vymazání, ale virový útok či vyhoření zdroje může data zničit na obou místech současně.
5) Je dobré si vytvořit dvě záložní kopie a dát je na různá místa, minimalizuje se tím riziko ztráty dat živelnou pohromou, krádeží nebo ztrátě díky selhání tohoto média (díky vadnému barvivu v sadě DVD jsem po třech týdnech přišel o 40 GB dat).
6) Záložní kopie skladovat v pokojové teplotě na místě chráněném před přímým slunečním světlem (platí hlavně pro CD, DVD), žárem, prachem, magnetickým polem a náhodným mechanickým poškozením.
7) I pomocí základních nástrojů ve Windows (NT Backup) a Task Scheduleru (Plánovač úloh) lze vytvořit základní automatické zálohování.
8) V případě nouze lze k zálohování využít i freemailových velkokapacitních serverů (www.gmail.com). Jejich velikost schránky pro uživatele dnes již přesahuje 2 GB, povolená velikost příloh se pohybuje v řádech MB, spolehlivost služby je dostatečná (rozhodně více než používání disket). V případě nedůvěry v tyto neplacené volně dostupné služby není nic snazšího než před odesláním tyto dokumenty nějak zašifrovat / ochránit kódem (např. s použitím komprimačního programu jako WinRAR lze data ochránit kódem a ještě k tomu zapakovat během chvilky).

Běžně dostupná místa pro ukládání záloh pro každého:

diskety, CD, DVD, USB-HDD, USB-FLASH klíčenky a jiné paměťové karty, Mp3 přehrávače, FTP servery, emailové servery.

Poznámka na závěr:

Výdaje na ukládání dat v podnicích teď tvoří víc jak polovinu výdajů na IT a podle IDC (Industrial Development Corporation) se v letošním roce dostanou až na 75 % celkových výdajů na IT; náklady na správu dat se odhadem pohybují od 3,5 dolarů za rok na každý gigabyte podle sdružení SNIA (Storage Networking Industry Association) až po 13 dolarů podle Yankee Group.

4.6 (Medové hrníčky) Honeypots

V teorii tento nápad „decoy“ aplikací již nějakou dobu existuje, v praxi se ale začal používat až nedávno. Myšlenka medových hrníčků je založena na vytvoření „falešných” IS, které nemají žádné zabezpečení a dění na těchto systémech je pozorně sledováno.

Honeypoty jsou systémy, které mají za úkol vytvořit dojem, že nejsou řádně zabezpečeny a že jsou na nich "zajímavá" data, nebo že jejich kompromitací získá útočník strategický přístup do vnitrofiremní sítě. Ve skutečnosti ale na těchto strojích nejsou důležitá data žádná, nebo se jedná o data záměrně změněná.

Honeypoty se dají využít k dosažení následujících cílů:

- chceme mít přehled a možnost studovat nové metody útoků, chování útočníků, virů, červů atd.,
- máme podezření, že se nás někdo snaží kompromitovat zveřejněním interních informací, proč je někomu takřka bez námahy neposkytnout a zjistit přitom, o koho se jedná,
- v neposlední řade tyto systémy dobře slouží jako alarm a na odlákání pozornosti. Útočník, který se zabývá našimi nastraženými systémy, nemá čas hledat ty skutečné a útočit na ně a my můžeme dočasně zvýšit bezpečnost provozu dat na síti skutečné, např. zakázáním nejméně zabezpečených a nedůležitých služeb.

Existují dvě základní koncepce při vytváření honeypotů. Pokud je útoků na naši organizaci mnoho a my chceme monitorovat pouze reálné útoky, průzkumy či nové viry, vytvoříme takzvaný **"produkční" honeypot**. Tento typ honeypotu se vyznačuje tím, že není veden v DNS, nevedou na něj žádné hypertextové odkazy ani jiné odkazy. Jeho hlavní výhodou je naprosto nulové množství falešných poplachů. Za tímto typem honeypotu stojí myšlenka, že na systém, který neposkytuje žádné služby (nekomunikuje s okolím) a nemá žádnou produkční hodnotu nemá nikdo důvod přistupovat - pak dojdeme logicky k závěru, že každý pokus o komunikaci s "produkčním" honeypotem lze chápat jako útok.

V případě, že se toužíme dozvědět co nejvíce o nových metodách útočníků, virů atd., zvolíme Honeypot „studijní“, který je v mnoha ohledech přesným opakem „produkčního“. V tomto případě totiž volíme co nejlákavější DNS názvy (intranet.firma.cz, mail.firma.cz apod.). Ve vnitřní síti pak používáme jména typu výplaty, personální, přehledy a jiné. Takto zvolenými jmény si jistě zajistíme dostatek materiálu pro další studium nepřátel.

Po stránce technické lze honeypoty provozovat na virtuálním stroji běžícím na dobře zabezpečeném systému, jež se stará o logování útočníka. Dále můžeme útočníkovi podstrčit skutečný nezabezpečený systém, u kterého budeme sledovat a vyhodnocovat veškerou síťovou

komunikaci. Asi nejpoužívanější možností, jak realizovat honeypot, jsou specializované SW simulující reálné HW a SW produkty (např. router Cisco, webservery apod.).

Z hlediska funkčnosti dělíme honeypoty do dvou základních skupin na **low-interaction** (často pouze přihlašovací prompt, či se jen tváří jako nějaká služba a neumožňuje sledovat chování útočníka po proniknutí do systému, + podstatně jednodušší zpracování nasbíraných údajů, - výrazně chudší na získané informace, není na čem pořádně sledovat útočníkovy postupy) a **high-interaction** (poskytne útočníkovi k dispozici nejen službu, či její část, ale celý stroj včetně operačního systému, + sledujeme přesně, co útočník děla, jak za sebou „zametá stopy“ atd., - pracnější vyhodnocování získaných informací). [I-09]

Seznam existujících „medových hrníčků“ je k dispozici na http://www.honeypots.net.

4.7 Další prostředky k snížení bezpečnostních rizik

4.7.1 Přístupové systémy

Přístupové systémy slouží k fyzické ochraně dat a dalších aktiv – aby se žádná neoprávněná osoba nedostala k fyzickým částem IS, diskům, zálohám. Přístupovým systémům byla věnována má předcházející práce [08].

4.7.2 Záplatování IS

Záplaty jsou opravné balíky vydávané výrobcem systému pro nově objevené bezpečnostní chyby v kódu. Protože tyto objevené chyby byly většinou někde zveřejněny, je jen otázkou času, než se objeví útok těchto děr využívajících. Záplatování lze nastavit jako plně automatický proces, nepřidělávající administrátorům žádnou další práci.

Jejich činnost není vždy stoprocentní (občas zadělají staré chyby a objeví se chyby nové, občas způsobí problematické chování celého systému, jako například letošní říjnové záplaty pro systém MS Windows [I-10]), ve finále se ale jejich používaní vždy vyplatí.

Záplaty a komerční X nekomerční programy

Společnost Symantec zveřejnila výsledky získané na základě analýzy *Internet Security Threat Report,* podle kterých výrobci komerčních produktů vydávají záplaty v reakci na novou hrozbu mnohem rychleji, než u open source programů (jako hlavní důvod pomalého uvádění záplat přitom uvádějí fakt, že vývojáře volně šířených programů k tomu nenutí žádné komerční páky). Podle zástupců firmy se navíc prodleva mezi objeveným slabým místem v programu a jeho následnou opravou neustále zvětšuje. V současnosti činí průměrně 54 dní.

Počet lidí dávají přednost open source programům (Mozilla Firefox, Open Office atd.) se přitom neustále zvyšuje. A čím více lidí bude tyto produkty používat, tím více se na tyto produkty budou hackeři zaměřovat - pokud se tento trend v rychlosti vydávání záplat u nekomerčních produktů nezmění, situace by se mohla stát až kritickou. [I-01]

4.7.3 Využití zabezpečených verzí protokolů

Tam, kde posíláme / přijímáme důvěrná data na / z internet-u, je vhodné použít zabezpečené komunikační protokoly zamezující odposlech dat během jejich přenosu.

Například klasický protokol pro přenos souborů FTP ve své nezabezpečené podobě během komunikace se vzdáleným počítačem nepoužívá žádné šifrování, veškeré příkazy protokolu, přenášená data, uživatelská jména, hesla cestují po síti v otevřené podobě. Proto se objevila jeho zabezpečená podoba s názvem Secure FTP. Tento protokol využívá bezpečnostního tunelu, vytvořeného protokoly SSH. Při použití tohoto protokolu se klient a server nejprve navzájem autentizují a veškerá další komunikace probíhá zašifrovaně.

Stejně tak při používaní HTTP protokolu je občas třeba, aby komunikace probíhala zabezpečeně (přístup do stravovacího systému přes internet, do emailu atd.) a naše důvěrné údaje necestovaly v otevřené podobě. Pro zabezpečení přístupu na webové stránky se používá speciální vrstva, protokol SSL. Stránky používající protokol SSL pak mají ve své adrese místo klasické HTTP adresu začínající HTTPS. Dalším takovým protokolem je například S-HTTP.

Co se týče vzdálené správy, místo klasického protokolu telnet se v dnešní době používá zabezpečeného protokolu SSH (secure shell).

Existují ale i řešení, pracující na mnohem nižší vrstvě, které dokáží chránit síťový provoz bez ohledu na podporu aplikací, například sada protokolů IPsec. Jedná se o sadu protokolů podporující zabezpečenou výměnu paketů na IP vrstvě. Tato technologie se dočkala širokého využití ve virtuálních privátních sítích (VPN).

Těchto zabezpečených protokolů by se dalo samozřejmě najít mnohem více. Pro základní představu by ale tato jejich ukázka měla být dostatečná.

4.7.4 Pár tipů k autentizaci a řízení přístupu

Sebelepší mechanismus pro ověřování totožnosti uživatele není nic platný, pokud není správně používán. Je třeba důsledně trvat na tom, aby přístup k počítači byl chráněn předepsaným způsobem. Tím je myšleno, aby zaměstnanci používali hesla zvolená podle daných pravidel, tyto hesla pravidelně obměňovali, nezapisovali je na papírky k monitoru atd..

V případě používání bezpečnostního předmětu (karty, tokeny, klíčenky atd.) by bylo „dobré“, aby ho nenechávali během dne volně u počítače, nemluvě po pracovní době (tomu se dá vyhnout pomocí použití stejného předmětu k docházkovému, přístupovému terminálu při vstupu / odchodu do / ze zaměstnání).

Co se týče řízení přístupu, tak pro systémy, kde se vyskytují počítačově „neoslovení“ lidé by mělo platit základní pravidlo - čím méně je uživatelovi dostupné, tím menší škody může svým ne / úmyslným konáním způsobit. Ideální je situace, kdy mu kromě poštovního klienta, aplikací nutných pro vykonávání činnosti, řádně zabezpečeného internetového prohlížeče a osobního adresáře není dostupné nic jiného a všechny další případné služby a programy by byly dostupné až po rozhovoru s osobou zodpovídající za bezpečnost daného IS.

Zcela jiná situace nastává ve firmách, kde se pohybují počítačově zdatní jedinci. Tam je třeba uplatnit mnohem citlivější přístup, případně více kompromisů, jinak se interní počítačová síť stane bojištěm uživatelů X správci systému. Přičemž při těchto pokusech o obcházení „nesmyslných“ bezpečnostních pravidel dochází k mnohem většímu riziku výskytu bezpečnostních incidentů, než kdyby správce v rozumné míře povolil nějaké ústupky.

Největší chybou správců / managementu je bezdůvodné zavádění nesmyslných restrikcí, např. zamezení přístupu na Internet, které nejenže zhoršují pracovní morálku, ale někdy i snižují samotnou možnou výkonnost (v případě zmiňovaného Internetu uzavřou cestu k velice cennému a aktuálnímu zdroji, zakázáním IM programů zamezí kontaktu se spřátelenými odborníky z diskusních fór atd.).

5. Modelové řešení zabezpečení IS/IT pro středně velkou organizaci

Poslední kapitola mé práce popisuje modelový návrh řešení zabezpečení IS/IT středně velké organizace. Pro návrh řešení jsem si zvolil konkrétní firmu, kterou je stejně jako v případě bakalářské práce firma BrukoN s r.o. - sériový výrobce kontejnerů.

K výběru stejné firmy jsem přistoupil z důvodu kontinuity - v bakalářské práci jsem se mimo jiné zabýval i fyzickou bezpečností firmy (přístupovými systémy), nyní bych rád tento model dále rozpracoval z pohledu zabezpečení IS/IT.

Návrh zabezpečení vyjde z analýzy současného stavu a nutných změn v reakci na aktuální dění na poli bezpečnosti IS/IT. V závěru jsou rozebrány přínosy ze zavedení těchto bezpečnostních opatření.

5.1 Stručná charakteristika podniku a současný stav

Firma BrukoN, spol. s r. o., vznikla v roce 1993 a od počátku se specializuje na sériovou výrobu kontejnerů pro přepravu a skladování materiálu, sutí, odpadů všeho druhu. Dnes již objemem výroby patří mezi zavedené firmy se značnými zkušenostmi v oboru. Firma zaměstnává 90 zaměstnanců, z toho 77 pracuje ve výrobě a 13 v úseku správním. BrukoN, spol. s r.o. sídlí v části bývalého továrního komplexu ve vesnici Smidary; firmě z tohoto komplexu patří dvě budovy - výrobní hala a budova pro administrativní účely.

Výrobní hala obsahuje výrobní plochu (výbava: vrtačky, svářečky, nůžky na plech apod.), skladiště a barvírnu.

V administrativní budově se nacházejí kanceláře zaměstnanců ekonomicko-správního úseku, kancelář majitele, převlékárny se skřínkami pro zaměstnance, servrovna, toalety, umývárny, kuchyňka a tři plně vybavené obytné místnosti pro zahraniční zaměstnance. Ekonomicko-správní úsek a kancelář majitele leží v samostatném křídle budovy.

Z důvodu zachování přijatelného rozsahu práce jsem se rozhodl vynechat podrobnější popis činnosti firmy spolu s plánkem celého komplexu. Pro další části návrhu tyto údaje nejsou nezbytné, navíc jsou již všechny obsaženy v mé předcházející práci [8].

Současný stav IS/IT

Firma ke své činnosti využívá tyto programy: jednoduché skladové hospodářství, docházkový (spojený s modulem pro generování mezd) a přístupový systém, účetnictví, správu technické dokumentace, jednoduchý CRM systém. Tyto systémy běží na dvou serverech v servrovně. Přičemž počítač obsahující technickou dokumentaci slouží též jako tiskový server (firma vlastní dvě tiskárny - na výkresy a smlouvy). Přístup ke službám těchto serverů mají všichni administrativní pracovníci. Tiskárny pro výkresy a smlouvy jsou k němu připojeny také. Ke spojení s vnějším světem (dodavateli, partnery) donedávna sloužilo vytáčené připojení, které bylo nahrazeno 24/7 připojením. Veškeré části IS (kromě docházkových / přístupových terminálů a notebooků majitele a mistra) se nacházejí v ekonomicko-správní části administrativní budovy. Kromě zmiňovaných dvou serverů tvoří IS firmy dalších deset stolních počítačů a dva notebooky. Všechny tyto stanice pracují pod operačním systémem Microsoft Windows (ve verzi NT, 2000 či XP). Jednotlivé stanice nejsou zajištěny, pošta je ukládána na každé stanici, není centrální poštovní server. Lokální síť je ethernetová, centrálním bodem je rozbočovač, propojení je realizováno přes UTP.

Stávající zabezpečení představuje nainstalovaný antivirový program a základní firewall na server zprostředkovávající spojení do internetu. Vybraná sdílená data jsou pravidelně automaticky zálohována na náhradní disk ve stejném serveru, většinu záloh vlastní práce si zaměstnanci dle svého uvážení pořizují sami (diskety, některé počítače jsou vybaveny vypalovacími mechanikami). Při problémech s OS jednotlivých počítačů dochází k ruční reinstalaci. Servrovna je vybavena klimatizací (odstranění tepla a vlhka).

Poslední dobou se díky vzrůstajícímu objemu výroby a vyšším nárokům na administrativní pracovníky začali množit neúmyslné chyby v práci (např. mazání nesprávných souborů), opomenutí v zálohování. Díky nově pořízenému neustálému připojení k Internetu a umožnění vstupu všech počítačů do této sítě se organizace také začala potýkat se škodlivým softwarem v mnoha jeho podobách (hlavně prostřednictvím elektronické pošty), který způsobil nedostupnost některých stanic. Také se vyskytl problém s tím, že jedna stanice sloužila nevědomě jako odesílatel spamu a ISP hrozil odpojením. Pracovníci nejsou příliš zruční ve správném užívání PC, většina PC je nezaheslovaných, či používá „slabá“ hesla. Operační systémy a jejich komponenty nejsou aktualizovány. Díky pracím v blízké rozvodně se začínají množit krátkodobé výpadky dodávky elektrické energie, způsobující dočasnou nedostupnost systému.

K žádnému úniku / ztrátě citlivých informací zatím naštěstí nedošlo, dostupnost služeb systému byla doposavad přijatelná, přesto ale vedení firmy dospělo k rozhodnutí zavést bezpečnostní opatření, které by snížilo množství / dopad bezpečnostních incidentů a zajistilo maximálně možnou spolehlivost systému.

5.2 Úvodní část návrhu řešení

Návrh řešení zlepšení zabezpečení IS/IT je pouze modelový, do řešitelské etapy nevstupuje. Pro základní představu o řízení bezpečnosti IS/IT ve firmě by ale měl být dostačující.

Jak už bylo zmíněno v první části práce, základním dokumentem každé společnosti z hlediska počítačové bezpečnosti je takzvaná bezpečnostní politika. První část politiky se věnuje popisu stávajícího systému (viz. podkapitola v 5.1 - současný stav IT). Dále je třeba určit, kdo bude za řízení firemní informační bezpečnosti zodpovědný.

5.2.1 Personální zajištění

Před samotným započetím vlastních prací na IS/IT je třeba se rozhodnout, kdo bude mít zajištění daného řešení na starosti (kdo se bude zodpovídat vedení společnosti, kdo bude mít rozhodovací pravomoci). Je samozřejmé, že ve finále se o bezpečnost bude starat někdo z IT oddělení (správci, administrátoři), ti budou konfigurovat dané počítače a hlídat aktualizace atd.. Nyní je třeba ale vybrat někoho, kdo bude toto zavádění bezpečnosti a následné udržení zavádět.

Ve firmě této velikosti a závislosti na IT/IS je nejlepším možným řešením outsourcing celého IT oddělení. V Hradci Králové se nacházejí odborné firmy, které snadno zajistí kvalifikované pracovníky, mohou jednoduše sledovat běh stanic a serverů přes VPN, případně na dálku provádět i některé administrátorské zásahy. Navíc v případě havárie, kdy její následky nebude možné odstranit na dálku, dokáží na místo dorazit v řádově desítkách minut. Prvotní návrh zabezpečení však navrhnu sám. Hlavní komunikaci s odborníky bude obstarávat majitel firmy, který též zajistí, aby nové bezpečnostní nařízení a směrnice zapadly do celkové bezpečnostní politiky firmy.

Poznámka:

Možností outsourcingu bezpečnosti IS/IT a ne / výhod tohoto řešení pro společnost jsem se v analytické části podrobněji nezabýval. Tato problematika je přehledně popsána v [1].

5.2.2 Analýza rizik

Před návrhem nových opatření je třeba nějakým způsobem zjistit co a proti čemu chceme chránit. K tomu slouží analýza rizik. Díky poměrné jednoduchosti IS firmy BrukoN, spol. s r. o. a nižší závislosti na něm v tomto případě postačí kombinovaná metoda analýzy s prvky základního a neformálního přístupu, která se bude pouze volně řídit známými a zavedenými postupy, ale hlavní slovo bude mít zkušenost osob na této analýze pracujících.

K tomu, aby bylo možno určit vhodné metody ochrany, je ale nejprve třeba zmapovat celý informační systém a **identifikovat jeho aktiva.**

V případě IS firmy BrukoN takovými aktivy jsou např.: docházkový systém, výstupy docházkového systému, konfigurační soubory docházkového systému, databáze zaměstnanců, přístupový systém, konfigurační soubory přístupového systému, výstupy přístupového systému, program pro manipulaci s technickými výkresy, technické výkresy, zákaznické databáze, elektronická pošta, pevný disk počítače 1,2.., pevný disk se zálohou, cd se zálohou, stanice 1,2..., router, UTP 1,2... apod..

Po identifikování těchto aktiv je třeba **sestavit seznam hrozeb** vyplývající z prostředí, ve kterém systém pracuje a určit pravděpodobnost uplatnění této hrozby. V tomto případě pro menší firmy se většinou používá intuitivní vyhledávání rizik, kdy se načrtnou všechny situace, které mohou v tomto IS nastat (co když dojde k selhání pevného disku, co když vir zničí data na této stanici a pod.). Anebo se pro inspiraci vezme seznam hrozeb z nějaké co do velikosti a zaměření podobné firmy.

Na tomto místě nezbývá než upozornit, že tento způsob získání seznamu hrozeb je použitelný pouze pro malé IS, nebo pro organizace s malou závislostí na těchto IS. Čím více prvků daný IS má, tím větší je šance, že dojde k přehlédnutí nějaké hrozby, a zároveň tím menší je šance, že nalezneme jiný seznam přesně pasující na naši organizaci.

Nyní tedy existují dva seznamy, seznam hrozeb a seznam aktiv a můžeme přistoupit k **vlastní analýze rizik.** Při vlastní analýze procházíme jednotlivá aktiva a rozhodujeme, které hrozby se na konkrétní aktivum vztahují. K této dvojici se ještě obvykle přiřazuje pravděpodobnost, s jakou ke konkrétní hrozbě danému aktivu dojde a škoda, kterou by daná hrozba způsobila.

Tabulka číslo 2: Ukázka z analýzy rizik firmy BrukoN, spol. s r.o.

Aktivum	Hrozba	Pravděpodobnost	Dopad	Riziko
zálohy	zcizení	příležitostná	kritický	nepřijatelné
zálohy	zničení při přírodní katastrofě	nepravděpodobná	vážný	poškozující
logy z doch. systému	smazání	příležitostná	nevýznamný	zanedbatelné
technické výkresy	okopírování	málo pravděpodobné	kritický	nepřijatelné
OS PC1 (Win 2000)	napadení virem	pravděpodobná	vážný	nepřijatelné

Zdroj: Vlastní tvorba

Na základě pravděpodobnosti a odhadované škody dojde k vybrání aktiv, která je třeba chránit (nepřijatelné nelze tolerovat, musí být odstraněné; poškozující je vhodné odstranit, ale je třeba posoudit náklady s tím spojené apod.).

Zde bych znovu rád připomněl, že prostředí, ve kterém se IS nachází, není statické. Mění se hrozby, pravděpodobnosti (například postavení přehrady sníží nebezpečí záplav apod.), aktiva, finanční hodnota aktiv. Tuto analýzu je tedy třeba opakovat.

5.3 Návrh bezpečnostních opatření

Díky výstupům získaným z předcházejících částí nyní můžeme přistoupit k zabezpečení IS firmy BrukoN, spol. s r.o.. Ochrana by měla být navržena pro každou dvojici aktivum-hrozba, ale často dojde k situaci, kdy jedno použité bezpečnostní opatření řeší ochranu více takových dvojic (antivir nasazený na ochranu OS zabezpečí i všechny ostatní programy pod tímto OS nainstalované apod.). Ideálním postupem pro zabezpečování je tedy postup „shora dolů“ (od základního k podrobnějšímu).V praxi je ještě nutné ke každému opatření přidat odhadovanou částku na jeho pořízení a udržení (důležité pro schvalovací fázi BP).

Následující část stručně popisuje proces zavádění bezpečnostních opatření, rozdělených podle jednotlivých složek bezpečnostní politiky.

5.3.1 Fyzická bezpečnost

Fyzická bezpečnost se zabývá ochranou před přírodními katastrofami (povětrnostními vlivy, záplavami, požáry), ochranou objektů, bezpečným uložením nosičů dat a jejich bezpečnou likvidací, zásadou výstavby objektů a technickým zabezpečením provozu.

IS firmy BrukoN, spol. s r.o. se nenachází v záplavové zóně, nejbližší vodní tok je příliš daleko na to, aby mohl působit nějaké reálné nebezpečí, vodovodní rozvody jsou v pořádku. Jako prevence budou veškeré počítače umístěny na vyvýšených místech, kabeláž povede lištami u stropu, disky všech počítačů budou umístěny do výměnných rámečků. V případě nenadálé události je sestaven havarijní plán, jehož první částí je přenesení do bezpečí aktuálních záloh (archivní data má majitel společnosti uloženy u sebe doma), dále záchrana dalšího vybavení od toho nejhodnotnějšího po postradatelný.

Administrativní budova splňuje požadavky dle ČSN 730802 požární bezpečnost staveb - nevýrobní objekty, v budově je nainstalována elektronická požární signalizace.

Problematika ochrany objektu proti vloupání a omezení pohybu pracovníků v rámci firmy byla popsána v bakalářské práci [08].

Pro bezpečné uložení nosičů týdenních záloh slouží masivní trezor (došlo i k změně metody pořizování záloh, více viz kapitola 5.3.4 Technická bezpečnost), k ničení neelektronických

nosičů dat (papírové dokumenty) budou pořízeny kancelářské skartovací stroje, přičemž zaměstnanci budou poučeni o jejich využívání (jedno z mnoha opatření režimové bezpečnosti).

Aby byl zajištěn co nejstabilnější běh IS (technické zabezpečení provozu), je třeba také zajistit pokud možno nepřetržitou dodávku elektrické energie (při stabilním napětí a frekvenci). Pro kratší výpadky elektrické energie a pro vyrovnání případných kolísání budou pro běh serverů a vybraných stanic pořízeny UPS spolu s přepěťovými ochranami a filtry, zakoupení agregátu na výrobu elektrické energie pro případ delších výpadků je ve fázi schvalování. Nainstalovaná klimatizace má dostatečný výkon, zde není třeba cokoli měnit.

5.3.2 Personální bezpečnost

Personální bezpečnost zajišťuje ochranu informačního systému před nežádoucím vlivem lidského faktoru.

Ve firmě BrukoN, spol. s r.o. se na administrativních pozicích nenacházejí lidé s pokročilou uživatelskou znalostí PC. Přitom spolehlivost těchto zaměstnanců je vysoká, s majitelem firmy mají výborné vztahy. Hlavním cílem tedy bude omezit práva uživatelů tak, aby nechtěně nezpůsobili nějaký bezpečnostní incident.

Předně je třeba vymezit jejich pohyb po síti a ke službám programů běžících na serverech. Prioritní je osoba majitele, jeho stolní počítač a notebook bude mít zpřístupněny všechny tyto služby v plném rozsahu. Další osoby budou mít zpřístupněny pouze ty služby, které potřebují ke své práci (vedoucí výroby přístup k technické dokumentaci, tiskárnám, aktuálním výstupům z docházkového systému, elektronické poště apod.).

Co se týče lokálních stanic, nejlepší metodou je nejprve nainstalovat OS, poté provést spolu s daným uživatelem instalaci aplikací potřebných pro výkon povolání, nakonfigurovat funkce a vzhled OS a programů tak, aby neztěžovali dané osobě práci, případně přidat další programy na přání pracovníka, které nejsou v rozporu s jeho pracovní náplní / zákonem a poté veškeré další změny zakázat. Jakékoli jiné zásahy do systému budou umožněny až po posouzení majitelem (či jiné pověřené osoby) a následné konzultaci s pracovníkem bezpečnostní firmy.

Po instalaci a zkušebním provozu zavedených bezpečnostních opatření je třeba uspořádat školení vysvětlující nová pravidla, poučit zaměstnance o zásadách chování (tvoření hesel, chování v systému apod. - součástí režimové bezpečnosti). V následujících týdnech je nutné na dodržování těchto nových pravidel dohlížet.

5.3.3 Režimová bezpečnost

Obsahem režimové bezpečnosti je sada bezpečnostních opatření, zásad, metod a postupů, která bere v úvahu všechny možné reálné situace včetně bezpečnostních incidentů (havárie, útoky zvenčí / zevnitř, další hrozby) a katastrofických scénářů a dokáže zachovat za těchto okolností funkčnost a provoz IS / minimalizovat dobu nedostupnosti. Pomocí této bezpečnosti se také prosazuje respektování právních norem a zákonů, bezpečnostních standardů a normativů v provozu informačního systému. Režimová opatření mají podobu nařízení a směrnic a konkrétně pokrývají např. následující situace / procesy:

Přístup do budov jednotlivých pracovníků a způsob kontroly jejich totožnosti byl stanoven v [8]. Přístupová práva ke službám IS byla vytvořena pomocí metody vše zakázat a poté postupně povolovat programy nezbytné pro výkon povolání, následně po konzultaci je zde možnost za dohledu odpovědné osoby instalace dalších nezávadných aplikací. Zakázány jsou také veškeré další zásahy do systému - ať už do HW či SW. Stejná pravidla platí pro připojení nového PC. Nové účty vytváří pouze pracovník bezpečnostní firmy. Při případném odchodu zaměstnance majitel nahlásí tuto změnu a bezpečnostní firma zruší veškerá práva pro daný účet. Pro přihlašování do systému byly stanoveny požadavky na délku a složitost hesla. Kromě důkazů znalostí je ještě nutné svoji totožnost dokázat pomocí důkazu vlastnictvím (čipová karta). V případě opuštění pracoviště na dobu delší než několik minut je nutné tuto kartu vzít sebou (toto zaručuje použití stejné karty pro docházkové, přístupové systémy). Při ztrátě karty dojde k odebrání jejích přístupových práv do systému, při pokusu o její použití systém vyšle skryté upozornění majiteli a bezpečnostní firmě.

Programové vybavení stanic bude pravidelně aktualizováno (jednou denně bude provedena kontrola, zda nejsou k dispozici nové aktualizace, v případě nové bezpečnostní hrozby častěji).

Pro šifrovaná data jsou stanoveny odpovídající metody generování a délka klíče, přičemž tyto klíče bude mít k dispozici pouze majitel firmy a pověřený pracovník firmy řešitelské. Média budou viditelně označena datem vzniku, obsah bude určen názvem (je možno zvolit názvy s nulovou vypovídající hodnotou pro nezasvěcené). Pro ničení záznamů z těchto médií bude v případě přepisovatelných médií provedeno důkladné smazání, v případě nepřepisovatelných zničení (skartovací přístroje na data v neelektronické podobě, mechanické zničení CD / DVD). Dále je nutné definovat způsoby bezpečného zálohování dat a uložení záložních a archivních médií (viz. podkapitola 5.3.4 Technická a 5.3.1 Fyzická bezpečnost).

V případě bezpečnostního incidentu / havárie dojde ke kontaktu bezpečnostní firmy, která se nejprve pokusí o odstranění problému pomocí telefonu či přes vzdálenou správu. Pokud tento problém nelze řešit na dálku, dojde k vyslání pracovníka.

5.3.4 Technická bezpečnost

Jedná se o ochranu dat použitím odpovídajícího technického vybavení. Jinak řečeno, aby přes problémy s technikou nedošlo ke ztrátě integrity dat, či dokonce k nedostupnosti systému.

Základem stabilního chodu PC jsou kvalitní zdroje. Při slabém zdroji se objevují problémy se stabilitou, hrozí přetížení zdroje s jeho následným zničením, při kterém může dojít k poškození ostatních částí systému. Zde se při revizi používaných stanic přišlo na několik PC, jejichž zdroje byly původně určené pro jinou konfiguraci (bez nových disků, mechanik, karet apod.) a které pracovaly na hranici svých možností. V nejbližší době budou vyměněny za jiné s větším výkonem.

Další objevenou závadou byla zaprášenost vnitřku stanic, kde některé větráky byly doslova zalepeny prachem. Prach zároveň působí jako tepelný izolant, v extrémních případech může dokonce dojít k jeho vznícení. Přičemž zvýšená teplota komponent snižuje jejich životnost. I zde bude v nejbližší době provedeno kompletní vyčištění, při kterém zároveň dojde k výměně některých chladicích ventilátorů za pasivní pro celkové snížení hlučnosti stanice při stejně / více kvalitním chlazení. Toto čištění od prachu se bude opakovat každých šest měsíců.

Opomenout nelze ani pevné disky, které díky mechanickým součástkám patří mezi nejvíc poruchové součásti počítače. Všechny novější disky je již možné hlídat přes takzvané SMART atributy (Self-Monitoring, Analysis and Reporting Technology), které monitorují pevný disk a v případě podezření na zhoršení funkcí disku spustí poplach. Tato metoda ale není úplně spolehlivá, navíc ne všechny disky ve firmě toto sledovaní podporují. U stanic tedy řešení tohoto problému spočívá v zálohování systémové části pevných disků (kde je nainstalován systém a ostatní programy), dále vybraných míst pro ukládání pracovních dokumentů na nově pořízený zálohovací server. Stejně tak na zálohovací server budou pravidelně umísťovány data ze zbylých dvou serverů. Zálohovací server bude typu NAS.

Pro případ výpadku zálohovacího serveru a jeho vnitřní zálohy jsou ještě všechna důležitá data ukládána na disky DVD (jedině značky Verbatim, Imation, DVD +R či DVD-RAM). Periodicita zálohování bude v pracovní dny každou půlnoc plná záloha, přes den bude provedena

v době polední pauzy záloha nových / změněných dat ve vybraných adresářích (adresáře s dokumenty, pošta, data z docházkových, přístupových snímačů, technické dokumenty apod.).

Porucha ostatních komponent nezpůsobí vážnější ztrátu integrity dat / nedostupnosti systému, je možno je tedy z kontroly vyjmout, či kontrolu provést později.

5.3.5 Datová a programová bezpečnost

Nyní přichází na řadu zabezpečení dat před kompromitací, modifikací, zničením. Porušení důvěrnosti, integrity a existence dat hrozí odcizením záloh, neautorizovaným přístupem do systému, odcizením pevných disků obsahujícím data, zničením nosičů dat. Velice nebezpečné jsou škodlivé programy. Pozor je také třeba dát na data v neelektronické podobě.

Díky novému 24/7 připojení do internetu je hlavní pozornost třeba věnovat ochraně IS proti hrozbám přicházejícím zvenku. Základem je ke vstupnímu bodu do firmy pořídit kvalitní firewall a antivirový systém s modulem pro kontrolu příchozí pošty (dosud používaný antivirový systém byl shledán nevhodným - velké nároky na systémové prostředky, nemožnost vzdálené správy a nedostatečná rychlost aktualizací databáze při vypuknutí nových epidemií) a antispamovým filtrem. Pošta bude pro snadnější správu a údržbu centralizována na jednom ze serverů. Všechny stanice budou vybaveny osobními firewally a antivirovými programy s možností vzdálené správy. Samozřejmostí je aktualizace bezpečnostních záplat a nastavení automatického stahování aktualizací (viz. Režimová bezpečnost). Pro prohlížení internetových prezentací byl vybrán alternativní SW, místo Internet Exploreru dojde k instalaci Mozilly Firefox.

Veškeré zálohy budou šifrovány pomocí některého z osvědčených, volně dostupných řešení (například http://www.truecrypt.org/). Použita bude některá ze symetrických šifer (pravděpodobně 3DES). Klíč k těmto zálohám bude mít majitel a bezpečnostní firma. Stejnou metodou budou chráněny i zálohy na zálohovacím serveru, vybraná data na ostatních dvou serverech (dokumenty, technické výkresy) a adresáře s dokumenty na jednotlivých stanicích. Citlivá data z docházkových a přístupových systémů jsou chráněna sama o sobě příslušnými programy tak, aby splňovali jim určená kriteria. Stejně tak jsou předepsanou ochranou chráněna data určená pro elektronickou komunikaci s úřady (osobní údaje pro Českou správu sociálního zabezpečení apod.).

Zálohování, metoda ochrany dat před jejich zničením, bylo popsána v předcházejících kapitolách. Jen pro upřesnění, jako vhodný nástroj pro tyto zálohy byl vybrán program Norton Ghost od společnosti Symantec.

Ke zvýšení ochrany před neautorizovaným přístupem dojde k zavedení přísnějšího heslového režimu ve spojení s nutností autentizace přes čipovou kartu, kterou zaměstnanci doposud používali pouze pro docházkové a přístupové systémy (viz. Režimová bezpečnost).

Citlivá data v podobě papírových dokumentů nyní budou mimo pracovní dobu ukládána do trezoru, nepotřebné dokumenty budou skartovány, skartovací zařízení bude v každé kanceláři.

5.3.6 Komunikační bezpečnost

Při řešení komunikační bezpečnosti se vychází s předpokladu, že samostatný počítač je již zabezpečen, považuje se za důvěryhodný a řeší se pouze ochrana komunikačních cest a informací, které přenášejí.

Veškeré propojení místní sítě se nově místo UTP realizuje přes lépe chráněné STP, centrálním místem je přitom směrovač v servrovně (hvězdicová topologie, dvoubodové spoje). Tento směrovač bude filtrovat provoz po síti podle hardwarových adres síťových karet - propustí jen ty karty, které má ve své databázi. Doposavad užívaný rozbočovač byl vyřazen. Nepoužívané kabely budou od směrovače odpojeny. Proti neoprávněnému napojení jsou kabely chráněny lištami. Data probíhající po síti zatím nebudou nijak šifrována. Stejně tak emailová komunikace, pokud zákon (hlavně kontakt s úřady) nevyžaduje jinak, bude posílána jako otevřený text.

Do budoucna se zvažuje možnost pokrytí výrobní haly a administrativní budovy technologií Wi-Fi (budou se kupovat další notebooky, připojení po STP není tak pohodlné). V tom případě by došlo k zabezpečení této sítě podle doporučení z podkapitoly věnované bezdrátovým sítím (3.6.3 Wi-Fi).

5.4 Zhodnocení přínosů ze zabezpečení IS/IT

Zavedení / udržování výše popsaných bezpečnostních opatření má / bude mít za následek snížení rizika výskytů bezpečnostních incidentů. Došlo k zajištění ochrany proti velkému množství subjektivních i objektivních hrozeb, k pokrytí zranitelných míst. A pro případ, kdy by k nějakému bezpečnostnímu incidentu přeci jen došlo (ani sebelépe vypracovaná a dodržovaná bezpečnostní politika nezaručí naprostou bezpečnost informačního systému - riziko nikdy nelze úplně odstranit, lze ho jen snížit na nějakou míru, která je pro nás přijatelná), byly zavedeny mechanismy pro snížení jejich dopadů a pro rychlé uvedení systému zpět do provozu.

Zodpovězení otázky ekonomické návratnosti je u investic do zabezpečení IS/IT značně problematické. Na jedné straně dokážeme přesně vyčíslit částky, které potřebujeme pro zavedení a udržení jednotlivých bezpečnostních mechanismů. Na straně druhé máme většinou pouze

statistiky o počtu nově odhalených bezpečnostních hrozbách (v poslední době hlavně viry, červy, trojské koně, phishing), bezpečnostních incidentech a odhadovaných škodách, které tyto incidenty způsobily. Při podrobnějším pohledu na tyto statistiky si však nelze nevšimnout rostoucí tendence jak u hrozeb, tak incidentů. Bezpečnostní politika také pomáhá se zvýšením odolnosti IS proti objektivním hrozbám, jako jsou selhání techniky, přírodní katastrofy apod.. Z tohoto pohledu už tato prevence dostává úplně jiný rozměr a zabezpečení IS/IT se stává **nutným krokem a základním předpokladem pro udržení funkčnosti firemního IS.** [I-02], [07]

Jsem si vědom toho, že mnou popsaný náčrt řešení neřeší všechny otázky bezpečnosti a nezaručí stoprocentní spolehlivost. Navíc mnou navrhovaná opatření nebyla testována v reálném světě, takže pravděpodobně opomíjí některé skutečnosti (hrozby a zranitelná místa), které by přišly v potaz při dlouhodobějším využívání systému. Domnívám se však, že pro názornou ukázku toho, jak může takový proces řízení bezpečnosti IS/IT v organizaci probíhat, je tento model dostatečně ilustrativní.

Závěr

Z témat, které byly zpracovány v rámci diplomové práce, vyplývá, že problematika bezpečnosti informačních systému je značně složitá, přičemž tato složitost vyplývá z velké různorodosti používaných informačních systémů a dynamického rozvoje světa informačních technologií.

Práce si dala za cíl tuto problematiku přehledně zmapovat. V analytické části práce (kapitola 2-4) byly nejprve vysvětleny základní pojmy spojené s informační bezpečností včetně jednotlivých fází procesu řízení bezpečnosti. Další dvě kapitoly (3-4) byly zaměřené na vybraná aktuální bezpečnostní rizika a na postupy umožňující jejich snižování. Podkladem pro vypracování analytické části pro mě byly knihy, odborné diskuse, webové portály, webové prezentace institucí, papírová a elektronická periodika zabývající se touto problematikou.

Syntetická část práce je věnována modelovému řešení zabezpečení IS/IT v organizaci, kde při vypracování jsem vycházel z teoretických poznatků z analytické části.

Na závěr je třeba zdůraznit několik faktů, které vyplynuly z použitých pramenů a vlastní práce. Řízení bezpečnosti IS/IT je nákladná záležitost, která negeneruje žádné zisky. Smysl zabezpečení IS/IT spočívá v prevenci vzniku bezpečnostních incidentů a tím zamezení vzniku škod z těchto incidentů vyplývajících (viz. kapitola 2.3 Proč vůbec zabezpečovat IS/IT).

Škody vzniklé působením bezpečnostních incidentů nelze vždy přesně vyčíslit, zde se ale literatura (jmenovitě alespoň [01], [05], [07] a [12]) shoduje, že pokud k nějakému význačnějšímu bezpečnostnímu incidentu dojde, pak tyto škody značně převyšují náklady vynaložené na zabezpečení.

Studie dostupné na internetu spolu s tématickým zaměřením většiny bezpečnostních portálů ukazují, že řada majitelů - provozovatelů IS věnuje velké náklady na zajištění technických a programových bezpečnostních systémů, ale stále opomíjí vliv lidského faktoru, zaměstnanců. I to se v budoucnu bude muset změnit, pouhou technikou udržet bezpečnost IS nelze. [I-02], [I-12]

Bezpečnost IS, tak jak je konstatováno v předcházejících částech, také není něco, co lze jednorázově pořídit, a pak se o to již dále nestarat. Je to neustávající proces boje mezi útočníky na straně jedné a bezpečnostními experty na straně druhé, vyžadující neustálou pozornost. [12]

Navíc s tím, jak prvky IS pronikají do nových oblastí a stávají se součástí nejen technických zařízení, ale i běžnou součástí našich domácností a současně se zvyšuje integrace těchto systémů a roste jejich složitost, existuje reálná pravděpodobnost, že bezpečnostních incidentů bude neustále přibývat a škody z nich vzniklé se mohou zvyšovat.

Seznam literatury:

[01] DOSEDĚL, T. Počítačová bezpečnost a ochrana dat. 1. vyd. Brno: Computer Press, 2004. ISBN-80-251-0106-1.

[02] DOBDA, L. Ochrana dat v informačních systémech. 1. vyd. Havlíčkův Brod: Grada Publishing, 1998. ISBN-80-7169-479-7.

[03] KUCHAŘ, M. Bezpečná síť. 1. vyd. Havlíčkův Brod: Grada Publishing, 1999. ISBN 80-7169-886-5.

[04] Security Magazín. 2002-2004. Praha: FAMily media. ISSN 1210-8723

[05] HALOUZKA, J., RACKOVÁ, E. a SEIGE, V. Informační bezpečnost, příručka manažera. 1. vyd. Hradec Králové: DSM Tate International, 2001. ISBN 80-902858-4-8.

[06] DOSEDĚL, T. 21 základních pravidel počítačové bezpečnosti. 1. vyd. Brno: Computer Press, 2005. ISBN 80-251-0574-1.

[07] TUDOR, J. K. Information Security Architecture: An Integrated Approach to Security in the Organization. 1.vyd. Auerbach Publications, 2000. ISBN: 0-8493-9988-2

[08] KOMÁREK, V. Problematika identifikace osob v běžném provozu organizace. [bakalářská práce.] Liberec: Technická univerzita v Liberci – Katedra informatiky, 2003.

[09] ČSN ISO/IEC TR 13335. Informační technologie - Směrnice pro řízení bezpečnosti. Český normalizační institut. 1999

[10] PC World Security. 2004-. Praha: IDG Infotainment. ISSN 1214-794X

[11] MITNICK, K., SIMON, W. The Art of Deception: Controlling the Human Element of Security. 1. vyd. USA: Wiley, 2002. ISBN 0-471-23712-4.

[12] TIPTON, H., KRAUSE, M. Information Security Management. 5.vyd. USA: Auerbach Publications, 2003. ISBN 0-8493-1997-8.

Další zdroje:

[I-01] Novinky [online]. [cit. 17.10.2005]. Dostupné z: http://www.novinky.cz/internet/

[I-02] Sans [online]. [cit. 17.10.2005]. Dostupné z: http://isc.sans.org/

[I-03] DigiWeb [online]. [cit. 17.10.2005]. Dostupné z: http://digiweb.ihned.cz/

[I-04] TechWorld [online]. [cit. 17.10.2005]. Dostupné z: http://www.techworld.com/security

[I-05] Živě [online]. [cit. 17.10.2005]. Dostupné z: http://www.zive.cz

[I-06] Crypto-World [online]. [cit. 17.10.2005]. Dostupné z: http://crypto-world.info

[I-07] NBÚ [online]. [cit. 24.10.2005]. Dostupné z: http://www.nbu.cz

[I-08] Storage [online]. [cit. 06.11.2005]. Dostupné z: http://www.storage.cz

[I-09] SystemOnLine [online]. [cit. 06.11.2005]. Dostupné z: http://www.systemonline.cz

[I-10] Technet [online]. [cit. 11.11.2005]. Dostupné z: http://technet.idnes.cz/

[I-11] Štít bezpečí [online]. [cit. 17.10.2005]. Dostupné z: http://www.stitbezpeci.cz/

[I-12] IBM [online]. [cit. 17.10.2005]. Dostupné z: http://www.ibm.com/

[I-13] Security portál [online]. [cit. 21.11.2005]. Dostupné z: http://www.security-portal.cz

[I-14] Anti-Phishin Working Group [online]. [cit. 21.11.2005].
Dostupné z: http://www.antiphishing.org/

[I-15] IMlogic [online]. [cit. 21.12.2005]. Dostupné z: http://www.imlogic.com/

Slovníček pojmů

Exploit - Kód (program) využívající známou bezpečnostní díru (v operačním systému, v prohlížeči atd.) ke spuštění škodlivého kódu (např. bez vědomí uživatele). Proti exploitům se lze efektivně bránit používáním aktuálních verzí jednotlivých produktů. Konkrétně v případě OS Windows a Internet Exploreru lze toto zajistit prostřednictvím průvodce na stránkách windowsupdate.microsoft.com.

Wetware – 1. Lidský nervový systém, jako protiklad k počítačovému hardware či software. 2. Lidské bytosti (programátoři, operátoři, administrátoři) svázané s počítačovým systémem, jako protiklad k systémovému hardware či software.

Seznam příloh:

Příloha č. 1: Pojmy spojené s analýzou rizik

1.1 Hrozba

Zranitelná místa jsou vlastnostmi (součástmi) IS, jejichž existence způsobuje, že některé vlivy v jeho prostředí pro něj představují hrozby. Pojmem **hrozba** označujeme **možnost využití zranitelného místa IS k útoku na něj** - ke způsobení škody na firemních investicích (aktivech). Základní dělení hrozeb je na **hrozby plynoucí z lidského faktoru** (subjektivní) a **objektivní** (tedy na náhodné a úmyslné okolnosti). Objektivní hrozby se dále dělí na fyzikální, fyzické / přírodní, technické a logické (příklady viz. zranitelná místa). Subjektivní se potom dělí na úmyslné a neúmyslné (působení neškoleného uživatele, chyba správce apod.).

Charakteristikou hrozby je její zdroj, motivace potenciálního útočníka, frekvence a kritičnost uplatnění hrozby. Kromě toho lze hrozby dělit podle částí systému, kterou ovlivní (prostředí a infrastruktura, HW, SW, komunikace, dokumentace, personální atd.). [03]

1.2 Zranitelné místo

Zranitelné místo je slabinou IS využitelnou ke způsobení škod nebo ztrát. Na rozdíl od hrozeb se již jedná o **konkrétní vlastnosti daného systému**. Zranitelné místo samo o sobě není příčinou škody, ke škodě dochází tehdy, pokud je zranitelnost využita hrozbami.

Tyto místa jsou důsledkem chyb, selhání v analýze, v návrhu a / nebo implementaci IS, důsledkem vysoké hustoty uložených informací, složitosti softwaru, existencí skrytých kanálů pro přenos informace jinou než zamýšlenou cestou, neadekvátního provozu apod. Podstata zranitelného místa může být **fyzická** (např. umístění IS na místě, které je snadno dostupné sabotáži / vandalismu / špionáži, výpadky a kolísavé napětí atd.)**, přírodní** (záplavy, požár, zemětřesení, blesk)**, HW** (nedostatečná klimatizace v servrovně)**, SW** (příliš složité uživatelské rozhraní)**, fyzikální** (elektromagnetické vyzařování zařízení zpracovávajícího informace, útoky při komunikaci na výměnu zprávy, na spoje – odposlech na Wi-Fi sítích), **lidský faktor - personální** (největší podíl na zranitelnosti IS, více v sekci Útočníci), **organizační, administrativní, procedurální nebo informací.** [02]

1.3 Útočníci

Pojmem útočník označujeme toho, kdo útočí na IS. Dříve nebo později se s ním setká každý IS. Útočníky můžeme **dělit podle tří** základních **kriterií – stupně odbornosti vedeného útoku, povaze útoku a podle polohy útočníka vzhledem k systému.**

Útočníci podle stupně odbornosti

Podle odbornosti dělíme útočníky na **amatéry, hackery a profesionály.**

Amatéři

Nejméně nebezpeční jsou amatéři. Většina jejich pokusů spočívá v pokusech o využití známých a zveřejněných bezpečnostních děr, spouštění již zmíněných skriptů a programů určených na pokusy k prolomení do systému, skenování portů atd.. Hlavní motivací je u většiny zvědavost, zda opravdu se dá do systému nějakým způsobem vstoupit. Do této skupiny patří hlavně mladiství, počítačově nepříliš gramotní lidé apod.. Nemají znalosti, čas ani vybavení k provedení nějakého sofistikovaného útoku. K ochraně před tímto typem útočníků dostačují poměrně levná a snadno dostupná bezpečnostní opatření (záplaty pro MS Windows, zdarma dostupné firewally v základním nastavení atd.).

Hackeři

Jiná situace přichází s hackery (rozsekávač, průnikář). Hackeři jsou osoby s velmi dobrou znalostí oblasti IS/IT, jedná se často o studenty vysokých škol, správce sítí, administrátory atd.. Ti již dokáží napadnout systém poměrně nepříjemnými útoky. K těmto útokům mají také poměrně dost času. Jejich limitací však jsou prostředky a výpočetní výkon. Motivací je potom opět hlavně zvědavost, snaha si něco dokázat, či zvídavost. Obrana proti nim postačuje standardní, většina IS je proti těmto útokům chráněná, nebo se alespoň snaží být.

Profesionálové

Největší hrozbu pro IS představují útoky vedené profesionály. Rekrutovaní znalci svého oboru, vybaveni velmi dobrými znalostmi a prostředky, výpočetním výkonem a spoustou času. Proti jejich útokům většinou neustojí žádný IS, používají nové a neortodoxní metody a postupy. I jen pokusy o zabezpečení proti těmto typům útoků jsou velmi nákladné a složité. V běžné praxi na něj firmy většinou předem rezignují a doufají, že právě jim a jejich systému se tento útok vyhne. Motivace těchto lidí bývá různá. Do této skupiny se řadí jak nezávislí specialisté, tak nájemní zločinci a teroristé snažící se škodit za každou cenu. Vyloučit se nedají ani vládní organizace a tajné služby, ať už se jedná o organizace kteréhokoli státu.

Útočníci podle způsobu útoku

Útočníky lze rozdělit i podle cíle útoku, přesněji oblasti, kterou se při své činnosti zabývají, případně podle úmyslu, který svým útokem sledují. Rozeznáváme tři hlavní skupiny a to **hackery, crackery a sociální inženýry.** Trochu stranou jsou běžní **zloději**, kteří jdou

primárně po HW, nikoli po SW (neplatí vždy, odcizení záložních kopií či notebooku za účelem přístupu k datům není také nijak neobvyklé).

Hacker

Podle definice je **hacker** osoba, která své draze nabyté zkušenosti využívá altruisticky pro dobro všech. Celé dny stráví na internetu a vyhledává bezpečnostní díry a nedostatečně zabezpečené systémy. Pokud nějakou závadu objeví, nevyužije ji, ale nahlásí tuto skutečnost správcům daného IS / vývojářům a doporučí jim, jak ji nejlépe opravit. Na internetu lze dokonce nalézt kodexy, které dané chování přesně popisují.

Realita se však od této definice poněkud liší. Někteří hackeři chybu správcům / vývojářům opravdu nahlásí a dají mu před zveřejněním nějaký čas na nápravu, ale většina z nich chybu stejně zveřejní (ke zveřejnění použije například nějaká diskusní fóra s hackersko-crackerskou tématikou, www stránky apod.). Prakticky všichni hackeři chyb zneužijí, ne sice z hmotných důvodů, ale většinou pro posílení ega a zvýšení svého hackerského „ratingu“. Hackeři se také velice často svým úspěchem chlubí veřejně - každý z nás si vzpomene, kdy v rádiu či jiném médiu zaslechl / si přečetl zprávu o tom, že hackeři pronikli na stránky té a té organizace a přeměnili její webovou prezentaci atd.. O následky svých činů se tito jedinci již většinou nestarají - napadený měl přece dost času na nápravu.

Hackeři se často organizují do skupin, mnohdy s mezinárodní účastí (za všechny jmenujme alespoň kdysi nejznámější německý Chaos Club). Jejich organizace je většinou na velice dobré úrovni. Během roku probíhají dokonce různá hackerská klání, kdy se soutěží v počtu prolomených systémů za určitý časový úsek, vyměňují se informace a postupy apod.

Cracker

Cracker je člověk, který se zabývá prolamováním ochran počítačových programů a jejich následnou úpravou, tak aby tyto programy byly zbaveny všech proti-pirátských ochran (originální médium v mechanice při spouštění programu, HW klíč, sériová čísla, online registrace atd.) a byly volně šiřitelné přes scénu a její FTP a dále pak mezi běžné uživatele P2P sítí.

Rozdíl mezi crackerem a hackerem je ten, že cracker “láme“ ochrany programů na svém počítači, zatímco hacker je někdo, kdo útočí na IS vzdáleně. [01]

Každý systém je tak silný, jak silný je jeho nejslabší článek. V případě informačních technologií to pak platí dvojnásob. Pokud se podaří útočníkovi napadnout právě nejslabší článek, má vyhráno. Veškeré firewally, organizační politiky, šifrování, prostě bezpečnostní opatření jsou v tomto okamžiku k ničemu. Přitom není třeba ani kdovíjakých hackerských znalostí, aby člověk

dokázal tento nejslabší článek prolomit. Tím nejslabším článkem je totiž samotný člověk. A nejjednodušší (leč zároveň nejúčinnější) metoda útoku se jmenuje **Sociální inženýrství – umění klamu.**

Sociální inženýr

Sociálním inženýrům a sociotechnice je věnována podkapitola v třetí části práce (3.5 Sociotechnika).

Zloděj

Zloděje nějak blíže představovat nemá smysl. Odcizení výpočetní techniky a tím získání drahého HW a důvěrných dat je stálou hrozbou IS. Největším problémem těchto krádeží je to, že zálohy, notebooky apod. mají v sobě většinou data v nezašifrované podobě a tím k nim získá přístup i člověk v informatice ne právě zběhlý. Základním opatřením by proto mělo být šifrovaní a heslovaní odcizitelných komponent IS a řešení fyzického přístupu do organizace (více viz. [08]).

Útočníci podle polohy vzhledem k systému

Základní dělení útočníků podle polohy k systému je jasné. Útoky přicházejí buďto **z venku, nebo zevnitř.**

Útoky zevnitř

Útoky zevnitř přicházejí od samotných zaměstnanců pracujících s daným IS. Představují vůbec nejrizikovější faktor ohrožení bezpečnosti informací. Podle odhadů způsobují zaměstnanci zhruba 80% případů porušení ochrany. Zaměstnanci jsou potenciální hrozbou už proto, že mají největší znalosti o daném informačním systému, znají jeho funkčnost, zabezpečení i slabé stránky. Tak mají zajištěné ideální podmínky pro velmi citelné a záměrné zneužití informací.

Většina bezpečnostních incidentů způsobených vnitřními útočníky má ale povahu nechtěných nehod, které způsobuje různá kvalifikace zaměstnanců v oblasti informačních technologií (nechtěně smazané soubory, opomenutí zálohování, otevření infikovaného podezřelého emailu, neodborný zásah do HW stanice atd.). Nudící se personál, který z nudy zkouší dělat to, co nemá, dokáže také často způsobit neočekávané škody.

Existují ale i případy, kdy za vnitřními útoky stojí úmysl z důvodů nespokojenosti, zloby, či pomstychtivosti. Povýšení a zvýšení platu kolegy, napomenutí, vyhazov a s ním související snaha o získání co nejcennějších informací pro konkurenci - potencionálního nového zaměstnavatele, pomsta bývalého zaměstnance atd.. Největší nebezpečí pak představuje vědomý útok správce systému, který díky svým oprávněním může provést takřka cokoli.

Proti těmto typům útoků lze IS bránit dvěma přínosnými způsoby – zvyšováním loajality a spolehlivosti zaměstnanců. Větší loajalita zaměstnanců (plně v rukou managementu společnosti přes motivační odměny, sankce atd.) sníží počet úmyslných útoků a větší vzdělanost a uvědomění personálu (přes kvalitní školení a správnou konfiguraci celého systému) sníží počty útoků neúmyslných.

Třetí možností je co nejvíce omezit práva zaměstnanců při vstupu do IS - zakázat připojení k Internetu, filtrovat a propouštět pouze firemní emaily a zbytek dodávat alternativní cestou, zakázat jakékoli zásahy do stanice, sledovat zaměstnancům emaily a údery kláves, hlídat jejich činnost kamerovým systémem atd.. Tento způsob řešení problému ale není právě nejvhodnější, protože snižuje výkon i motivaci pracovníků a zhorší celkovou atmosféru ve firmě, navíc některé sledovací praktiky zaměstnavatelů jsou na hranici zákona (zajímavý článek o právu zaměstnance na soukromí, ochranu osobnosti a listovní tajemství v rámci pracovněprávních vztahů lze nalézt na [I-06], Ján Matejka, K oprávnění zaměstnavatele kontrolovat práci zaměstnance pomocí moderních technologií sešit 10/2003).

Poznámka:

Jsou IT oddělení bezpečnostní slabinou? Dle studie, vytvořené Tokijským Trend Micro, "věří" 39 procent zaměstnanců, že je jejich IT oddělení ochrání před viry, wormy, spyware, spamem, atd.. Zaměstnanci nemají zábrany klikat na neznámé odkazy či otevírat podezřelé emaily, poněvadž ví o různých bezpečnostních produktech, které IT oddělení instaluje na jejich pracovní stanice. Zaměstnanci především velkých společnosti si nedělají starosti se vzděláním v této oblasti a necítí žádnou zodpovědnost za bezpečnost svého počítače. Plně věří v IT oddělení, které je z případných problémů dostane. [I-01]

Útoky zvenčí

Vnější útočníci nemají fyzický přístup k vnitřní síti. Při svém útoku musejí překonat všechny překážky, které jim správci sítí kladou, počínaje firewally, konče například využitím zabezpečených protokolů pro všechny komunikační relace. Výhodou těchto útočníků je zhoršená vystopovatelnost – mohou být kdekoli a mohou se maskovat (např. přes proxyservery). A vzhledem k tomu, že útočník se může nacházet prakticky kdekoli, je i v případě jeho odhalení poměrně těžké prosadit jeho stíhání. V podstatě jedinou účinnou obranou proti vnějším útokům je důkladné zabezpečení počítačového systému.

Úplně nejnebezpečnějším typem útočníka je, když na vás útočí „celý svět“. Za celým útokem sice stojí zase většinou jen jeden člověk, který ale pro svůj úmysl předem ovládl a vytvořil síť vlastních počítačů, které potom vedou soustředěný útok na určené místo. Tento typ útoků se nazývá Distributed DoS (distribuovaný útok na dostupnost služeb). Hlavní nebezpečí těchto útoků spočívá v tom, že proti nim dosud neexistuje příliš účinná ochrana.

Příloha č. 2: Norma ISO/IEC TR 13335

Informační technologie - Směrnice pro řízení bezpečnosti IT

Část 1: Pojetí a modely bezpečnosti IT (ISO/IEC TR 13335-1)

Popisuje základní koncepce a modely používané pro správu bezpečnosti IT a její vztah ke správě informačních technologií. Definovány jsou zde rovněž základní pojmy bezpečnosti IT, které by organizace měla jednoznačně převzít. Otázka správných a přesných definic je v dokumentu důležitá. Tato první část je určena především pro členy bezpečnostní rady a pracovníky, kteří zodpovídají za bezpečnost IT a pro ty, kteří mají na starost celkový program bezpečnosti organizace.

Část 2: Řízení a plánování bezpečnosti IT (ISO/IEC TR 13335-2)

Popisuje řídící a plánovací aspekty IT. Je ji možné aplikovat na organizaci a řízení bezpečnosti IT v organizaci, definuje role a zodpovědnost jednotlivých zainteresovaných pracovníků. Je z ní možné čerpat pro definici cílů a prvků celkové bezpečnostní politiky IT v organizaci a bezpečnostní politiky jednotlivých systémů IT. Jsou zde vysvětleny významy různých analýz a přístupů k nim. Dále je zde popsán výběr bezpečnostních opatření a přijetí zbytkového rizika. V neposlední řadě je zde uvedeno plánování bezpečnosti, zavádění bezpečnostních opatření, výchovného programu a následné údržby, monitorování, kontroly plnění a řešení incidentů. Tato druhá část je určena pro vedoucí pracovníky z oblasti systémů IT organizace, a dále pro ty osoby, které zodpovídají za aktivity organizace, na kterých se IT podílí rozhodující měrou.

Část 3: Techniky pro řízení bezpečnosti IT (ISO/IEC TR 13335-3)

Popisuje nejdůležitější bezpečnostní techniky, uvádí jejich strukturu a kategorizaci. Podrobně jsou zde rozebrány způsoby provádění rizikové analýzy a volba a strategie této analýzy. Tato část je určena pracovníkům organizace, kteří se podílejí na životním cyklu projektů plánování, návrhů, implementace, testování, pořizování a provozu systémů IT z hlediska jejich bezpečnosti.

Část 4: Výběr bezpečnostních opatření (ISO/IEC TR 13335-4)

Předkládá doporučení na výběr bezpečnostních protiopatření v kontextu specifických potřeb organizace.

Příloha č. 3: Vybrané normy z oblasti bezpečnosti IT

ČSN ISO/IEC 2382-1:199x	Informační technologie - Slovník - Část 1: Základní termíny
ČSN ISO/IEC 2382-8:2000	Informační technologie - Slovník - Část 8: Bezpečnost
ČSN ISO/IEC 2382-14:199x	Informační technologie - Slovník- Část 14: Spolehlivost
ČSN ISO/IEC TR 13335-1:1999	Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 1: Pojetí a modely bezpečnosti IT
ČSN ISO/IEC TR 13335-2:2000	Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 2: Řízení a plánování bezpečnosti IT
ČSN ISO/IEC TR 13335-3:2000	Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 3: Techniky pro řízení bezpečnosti IT
ČSN ISO/IEC TR 13335-4:2002	Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 4: Výběr ochranných opatření
ČSN ISO/IEC 17799:2005	Informační technologie - Soubor postupů pro management bezpečnosti informací
ČSN ISO/IEC 9798-1:1999	Informační technologie - Bezpečnostní techniky - Mechanismy autentizace entit - Část 1: Obecný rámec
ČSN ISO/IEC 9798-2:2000	Informační technologie - Bezpečnostní techniky - Mechanismy autentizace entit - Část 2: Mechanismus používající symetrický šifrovací algoritmus
ČSN ISO/IEC 9798-3:1997	Informační technologie - Bezpečnostní techniky - Mechanismy autentizace entit - Část 3: Mechanismus používající algoritmus veřejného klíče
ČSN ISO/IEC 9798-4:2001	Informační technologie - Bezpečnostní techniky - Mechanismy autentizace entit - Část 4: Mechanismy používající kryptografickou kontrolní funkci
ČSN ISO/IEC 9798-5:2001	Informační technologie - Bezpečnostní techniky - Mechanismy autentizace - Část 5: Mechanismy používající techniku nulových znalostí
ČSN ISO 8372:1997	Zpracování informací - Módy činnosti pro 64-bitový algoritmus blokové šifry
ČSN 36 9796:2005	Informační technologie - Bezpečnostní techniky – Struktura detekce průniku do IT
ČSN ISO/IEC 9796:1996	Informační technologie - Bezpečnostní techniky - - Schéma digitálního podpisu umožňujícího obnovu zprávy
ČSN ISO/IEC 9796-2:2004	Informační technologie - Bezpečnostní techniky- - Schémata digitálního podpisu umožňující obnovu zprávy - - Část 2: Mechanismy založené na faktorizaci celých čísel
ČSN ISO/IEC 9796-3:2002	Informační technologie - Bezpečnostní techniky - Schémata digitálních podpisů umožňující obnovu zprávy - Část 3: Mechanismy založené na diskrétních logaritmech
ČSN ISO/IEC 9797-1:2001	Informační technologie - Bezpečnostní techniky - Kódy pro autentizaci zprávy - Část 1: Mechanismy používající blokovou šifru
ISO/IEC 9797-2:2000	Information technology - Security techniques – Message Authentication Codes (MACs) - Part 2: Mechanisms using a hash function
ČSN ISO/IEC 9979:2001	Informační technologie - Bezpečnostní techniky – Postupy pro registraci kryptografických algoritmů
ČSN ISO 10116:2000	Informační technologie - Bezpečnostní techniky – Módy činnosti pro n-bitovou blokovou šifru
ČSN ISO/IEC 10118-1:1996	Informační technologie - Bezpečnostní techniky – Hash funkce - Část 1: Všeobecně
ČSN ISO/IEC 10118-2:1996	Informační technologie - Bezpečnostní techniky – Hash funkce - Část 2: Hash funkce používající algoritmus n-bitové blokové šifry
ČSN ISO/IEC 10118-3:2000	Informační technologie - Bezpečnostní techniky – Hash funkce - Část 3: Dedikované hash funkce
ČSN ISO/IEC 10118-4:2001	Informační technologie - Bezpečnostní techniky – Hašovací funkce - Část 4: Hašovací funkce používající modulární aritmetiku
ČSN ISO/IEC 11770-1:1998	Informační technologie - Bezpečnostní techniky – Správa klíčů-Část 1: Struktura
ČSN ISO/IEC 11770-2:1999	Informační technologie - Bezpečnostní techniky – Správa klíčů - Část 2: Mechanismy používající symetrické techniky
ČSN ISO/IEC 11770-3:2002	Informační technologie - Bezpečnostní techniky – Správa klíčů - Část 3: Mechanismy používající asymetrické techniky
ČSN ISO/IEC 13888-1:2001	Informační technologie - Bezpečnostní techniky – Nepopiratelnost - Část 1: Všeobecně
ČSN ISO/IEC 13888-2:2001	Informační technologie - Bezpečnostní techniky- Nepopiratelnost - Část 2: Použití symetrických technik
ČSN ISO/IEC 13888-3:2001	Informační technologie - Bezpečnostní techniky - Nepopiratelnost - Část 3: Použití asymetrických technik
ČSN ISO/IEC 14888-1:2001	Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem - Část 1: Všeobecně

ČSN ISO/IEC 14888-2:2001	Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem - Část 2: Mechanismy založené na identitě
ČSN ISO/IEC 14888-3:2001	Informační technologie - Bezpečnostní techniky – Digitální podpisy s dodatkem - Část 3: Mechanismy založené na certifikátu
CSN ISO/IEC 15408-1:2001	Informační technologie - Bezpečnostní techniky - Požadavky pro hodnocení bezpečnosti IT - Část 1: Úvod a všeobecný model
ČSN ISO/IEC 15408-2:2002	Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 2: Bezpečnostní funkční požadavky
ČSN ISO/IEC 15408-3:2002	Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 3: Požadavky na záruky bezpečnosti
ČSN ISO/IEC TR 13594:2000 / ITU-T X.802:1995	Informační technologie – Bezpečnost nižších vrstev
ČSN ISO/IEC 9160-199x	Šifrování dat: Požadavky na interoperabilitu fyzické vrstvy
ČSN ISO/IEC 11577:1998	Informační technologie - Propojení informačních systémů - Bezpečnostní protokol sítové vrstvy
ČSN ISO/IEC 10736:1998	Informační technologie - Telekomunikace a výměna informací mezi systémy - Bezpečnostní protokol transportní vrstvy
ČSN ISO/IEC 7498-1:1997 /ITU-T X.800	Informační technologie - Propojení otevřených systémů - - Základní referenční model - Základní model
ČSN ISO/IEC 7498-2:1998	Systémy na Zpracování informací. Propojení otevřených systémů (OSI). Základní referenční model. Část 2: Bezpečnostní architektura
ČSN ISO/IEC 7498-4:1998 /ITU-T X.700	Systémy na spracovanie informácií. Prepojenie otvorených systémov (OSI). - Základný referenčný model. Časť 4: Základná štruktúra spracovania
ČSN ISO/IEC 9594-8:1999 /ITU-T X.509	Informační technologie - Propojení otevřených systémů - - Adresář: Struktura autentizace
ČSN ISO/IEC 10745:2000 /ITU-T X.803	Informační technologie - Propojení otevřených systémů - - Model bezpečnosti vyšších vrstev
ČSN ISO/IEC 10181-1 až 7:1998-1999 /ITU-T X.810-816	Informační technologie - Propojení otevřených systémů - - Bezpečnostní struktury otevřených systémů
ISO/IEC 11586-1 až 6:1996-7 /ITU-T X.830-835	Information technology- Open system interconnection - - Upper layer generic security
ČSN ISO/IEC 10164-7:1998 /ITU-T X.736	Informační technologie - Propojení otevřených systémů - - Management systémů: Funkce podávání bezpečnostních poplašných hlášení
ČSN ISO/IEC 10164-8:1998 /ITU-T X.740	Informační technologie - Propojení otevřených systémů - - Management systémů: Funkce bezpečnostního auditního záznamu
ČSN EN ISO/IEC 9646-1:199x	Informační technologie - Metodologie a struktura zkoušky shody - Část 1: Obecné pojmy
ČSN ISO/IEC 10021-1,2,4,5,8,9 /ITU-T X.400,402,411,413,435	Systémy zprostředkování zpráv (MHS)
ČSN ISO/IEC 12207:1997	Informační technologie - Procesy v životním cyklu softwaru
ČSN ISO/IEC 14598-5	Informační technologie - Hodnocení softwarového produktu
ČSN ISO/IEC TR 15504-1	Informační technologie - Posuzování softwarového procesu
ČSN ISO 8730:1996	Bankovnictví. Požadavky na autentizaci zpráv (bankovní služby pro velkou klientelu)
ČSN ISO 8731-1:1996	Bankovnictví. Schválené algoritmy pro autentizaci zprávy. Část 1: DEA
ČSN ISO 8731-2:1996	Bankovnictví. Schválené algoritmy pro autentizaci zprávy. Část 2: Algoritmus autentikátora zprávy
ČSN ISO 8732:1998	Bankovnictví- Správa klíčů (bankovní služby pro velkou klientelu)
ČSN ISO 9564-1:2005	Bankovnictví - Řízení a bezpečnost osobních identifikačních čísel (PIN) - Část 1: Základní principy a požadavky na online zacházení s PIN v systémech ATM a POS
ČSN ISO 9564-2:1996	Bankovnictví. Řízením a bezpečnost osobních identifikačních čísel. - Část 2: Schválené algoritmy pro šifrování PIN
ČSN ISO 9564-3:2005	Bankovnictví - Řízení a bezpečnost osobních identifikačních čísel - Část 3: Požadavky na off-line zacházení s PIN v systémech ATM a POS
ČSN ISO 9807:1996	Bankovnictví. Požadavky na autentizaci zprávy (bankovní služby pro drobnou klientelu)
ČSN ISO 10126-1:1996	Bankovnictví. Postupy pro šifrování zpráv (bankovní služby pro velkou klientelu). Část 1: Obecné zásady
ČSN ISO 10126-2:1996	Bankovnictví. Postupy pro šifrování zpráv (bankovní služby pro velkou klientelu). Část 2: Algoritmus DEA
ČSN ISO 10202-1:1994	Identifikační karty. Karty pro finanční transakce. Bezpečnostní architektura systémů finančních transakcí využívajících karty s integrovanými obvody. Část 1: Životní cyklus karty
ČSN ISO 10202-2:2005	Karty pro finanční transakce - Bezpečnostní architektura systémů finančních transakcí využívajících karty s integrovanými obvody - Část 2: Proces transakce

ČSN ISO 10202-3:1999	Karty pro finanční transakce - Bezpečnostní architektura systémů finančních transakcí využívajících karty s integrovanými obvody - Část 3: Vztahy mezi kryptografickými klíči
ČSN ISO 10202-4:2001	Karty pro finanční transakce - Bezpečnostní architektura systémů finančních transakcí využívajících karty s integrovanými obvody - Část 4: Bezpečné aplikační moduly
ČSN ISO 10202-5:2001	Karty pro finanční transakce - Bezpečnostní architektura systémů finančních transakcí využívajících karty s integrovanými obvody - Část 5: Použití algoritmů
ČSN ISO 10202-6:2001	Karty pro finanční transakce - Bezpečnostní architektura systémů finančních transakcí využívajících karty s integrovanými obvody - Část 6: Ověření držitele karty
ČSN ISO 10202-7:2001	Karty pro finanční transakce - Bezpečnostní architektura systémů finančních transakcí využívajících karty s integrovanými obvody - Část 7: Správa klíčů
ČSN ISO 10202-8:2001	Karty pro finanční transakce - Bezpečnostní architektura systémů finančních transakcí využívajících karty s integrovanými obvody - Část 8: Všeobecné zásady a přehled
ČSN ISO 11131:1996	Bankovnictví. Autentizace přihlášením
ISO 13569:1997	Banking and related financial services – Information security guidelines
ISO 13491-1:1998	Banking - Secure cryptographic devices (retail) - Part 1: Concepts, requirements and evaluation methods
ČSN ISO 13491-2:2004	Bankovnictví - Bezpečná kryptografická zařízení (bankovní služby pro drobnou klientelu) - Část 2: Kontrolní seznamy shody bezpečnosti pro zařízení používaná v systémech karet s magnetickým proužkem
ČSN EN ISO 11568-1:1997	Bankovnictví- Správa klíčů (bankovní služby pro drobnou klientelu) - Část 1: Úvod do správy klíčů
ČSN EN ISO 11568-2:1997	Bankovnictví- Správa klíčů (bankovní služby pro drobnou klientelu) - Část 2: Techniky správy klíčů pro symetrickou šifru
ČSN EN ISO 11568-3:1997	Bankovnictví- Správa klíčů (bankovní služby pro drobnou klientelu) - Část 3: Životní cyklus klíče pro symetrickou šifru
ČSN EN 1546-1:1999	Systémy s identifikačními kartami – Mezioborová elektronická peněženka - Část 1: Definice, pojmy a struktury
ČSN EN 1546-2:2000	Systémy s identifikačními kartami – Mezioborová elektronická peněženka - Část 2: Bezpečnostní architektura
ČSN EN 1546-3:2000	Systémy s identifikačními kartami - Mezioborová elektronická peněženka - Část 3: Datové prvky a výměny
ČSN EN 1546-4:1999	Systémy s identifikačními kartami – Mezioborová elektronická peněženka - Část 4: Datové objekty

ČSN ISO 9735:2003-2004 1-10	Elektronická výměna dat pro správu, obchod a dopravu (EDIFACT), Pravidla syntaxe aplikační úrovně

Příloha č. 4: Struktura a obsah bezpečnostní politiky, příklad

Struktura politiky fiktivní společnosti Abc nebyla vytvořena na základě žádného konkrétního standardu, ale podle autorů byla její praktická použitelnost ověřena na mnoha projektech. Vhodná především pro rozsáhlejší IS. [05]

1. Úvod

Slova managementu Abc o významu ochrany vlastních informací. Stručné vysvětlení postavení a významu bezpečnostní politiky pro společnost Abc.

2. Cíle a rozsah bezpečnostní politiky

Definice hlavních a dílčích cílů politiky může vypadat následovně:

Hlavním cílem bezpečnosti definované v bezpečnostní politice IS Abc je trvalé a kvalitní zajištění dostupnosti, důvěrnosti a integrity informací Abc pořizovaných, zpracovávaných, ukládaných a přenášených pomocí IS Abc tak, aby byla zajištěna podpora primárních činností a cílů Abc realizovaných s využitím IS Abc.

Dílčími cíli bezpečnostní politiky jsou:

- ► definování zásad informační bezpečnosti Abc ve formě množiny pravidel;
- ► popis způsobu řízení informační bezpečnosti formou definice rolí a odpovídajících pravomocí a zodpovědností;
- ► uvedení východisek, která mají rozhodující význam pro formulaci zásad a řešení informační bezpečnosti Abc;
- ► pozitivní působení na zvyšování bezpečnostního vědomí zaměstnanců Abc;
- ► vymezení klíčových pojmů v oblasti informační bezpečnosti.

Rozsah bezpečnostní politiky může být vymezen takto:
Bezpečnostní politika IS Abc se zabývá informacemi pořizovanými, zpracovávanými, ukládanými a přenášenými prostřednictvím IS Abc. Bezpečnostní politika je závazná pro všechny zaměstnance Abc a všechny externí osoby, které se k tomu smluvně zavázaly.

3. Charakteristika IS Abc

Informační technologie

Stručný výčet součástí, z nichž se skládá IS Abc. Popis je vhodné rozdělit například na tyto části: programové vybavení, technické prvky, rozvody. Následuje charakteristika počítačové sítě Abc a provozu IS. Pokud je to účelné, v této kapitole je potřeba vymezit pojem kritické systémy (například výčtem).

Informace v elektronické podobě

Kapitola definující, na které informace v elektronické podobě se politika vztahuje. Je možná použít definici širokou, zahrnující veškeré informace, nebo naopak určité typy informací z definice vyjmout.

4. Východiska bezpečnosti

Zde jsou uvedeny skutečnosti, které mají významný vliv na požadovanou úroveň informační bezpečnosti v Abc a které se promítají do bezpečnostní politiky IS Abc a do způsobu jejího naplňování.

Zákonné a podzákonné normy

Výčet zákonů a vyhlášek majících vztah k předmětu podnikání Abc a k oblasti informační bezpečnosti.

Strategie Abc

Stručná charakteristika podnikatelské strategie Abc.

Interní dokumenty

Výčet interních legislativních norem, které mají vztah k ochraně informací v Abc.

Smluvní vztahy
Mohou existovat uzavřené smlouvy, které ovlivňují obsah bezpečnostní politiky. Příkladem mohou být jednání s dceřinými (partnerskými) společnostmi o poskytování (a ochraně informací. Pokud taková smluvní ujednání existují, kapitola obsahuje jejich výčet a stručný popis.

Další východiska
Popis dalších východisek nezmíněných výše.

5. Pravidla a zásady bezpečnosti IS Abc

Kapitola obsahuje výčet všech hlavních bezpečnostních pravidel a zásad, jimiž se řídí bezpečnost IS Abc. Důležitý je použitý jazyk. Jednou možností je prostý direktivní výčet jednotlivých pravidel a zásad. V takovém případě jsou všechna pravidla na stejné úrovni - všechna jsou závazná.

Druhou možností je připuštění použití podmiňovacího způsobu v některých formulacích. Význam je potom následující:

- ► „mělo by" (resp. „nemělo by") - vyjadřuje požadavek, který by měl být splněn, jakmile to dovolí technické a organizační podmínky Abc;
- ► „musí" (resp. „nesmí") - znamená požadavek, jehož splnění je nezbytné pro zajištění bezpečnosti informací.

Fyzická bezpečnost, možný obsah kapitoly:

- ► definice citlivých prostor (místnosti) a definice požadavků na umístění zabezpečení těchto prostor (režim vstupů, umístění v budově, vzdálenost od nebezpečných provozů, požadavky na vybavení a zabezpečení, označení atd.);
- ► základní pravidla pro ochranu budov;
- ► pravidla týkající se elektrického napájení;
- ► fyzická ochrana nosičů informací;

Personální bezpečnost, možný obsah kapitoly:

- ► obecná pravidla personální bezpečnosti (obsah pracovní smlouvy, zástupnost osob, požadavky na popis pracovních míst, vzdělávání atd.);
- ► vznik pracovního poměru;
- ► ukončení pracovního poměru;

Administrativní a procedurální bezpečnost, možný obsah kapitoly:

- ► řízení přístupu k informacím;
- ► pravidla pro předávání informací a dat uvnitř Abc a mimo Abc;
- ► správa IS;
- ► změnové řízení;
- ► pravidla pro (interní) klasifikaci informací;
- ► audit IS;
- ► bezpečnostní dokumentace;
- ► havarijní plány;
- ► smluvní vztahy.

Komunikační bezpečnost a bezpečnost IS Možný obsah kapitoly:

- ► sledování činnosti uživatelů;
- ► zajištění integrity informací a IS;
- ► spolehlivost dostupných služeb;
- ► požadavky na zabezpečení dat;
- ► pravidla identifikace a autentizace;
- ► řízení přístupu.

6. Řízení bezpečnosti IS Abc

Kapitola popisuje strukturu bezpečnostního managementu, způsob zvládání bezpečnostních incidentů a postup testování bezpečnosti.

Bezpečnostní infrastruktura
Popis celkové struktury bezpečnostního managementu (schéma) včetně výčtu jednotlivých rolí.

Popis rolí, zodpovědností a pravomocí
Příklady rolí, které se mohou v bezpečnostní politice IS objevit:

- ► uživatel;
- ► externí uživatel;
- ► gestor informací (dat);
- ► gestor aplikace;
- ► vedoucí pracovník (člen managementu);
- ► správce systému;
- ► operátor;
- ► bezpečnostní správce;
- ► bezpečnostní manažer.

Pro každou roli je uvedena stručná charakteristika role plus uvedení seznamu povinností a pravomocí.

Řešení bezpečnostních incidentů
Bezpečnostním incidentem je myšlena jakákoli událost nebo činnost, která vede k podstatnému přímému či nepřímému ohrožení dostupnosti, důvěrnosti nebo integrity informací a dat zpracovávaných a ukládaných v IS. Rychlá a odpovídající reakce na incident je jedním z nejdůležitějších požadavků kladených na bezpečnostní management.

Kapitola obsahuje:
► netaxativní výčet příkladů bezpečnostních incidentů;
► kontaktní místa pro ohlášení incidentů;
► stanovení povinnosti všech zaměstnanců Abc reagovat na incident a podle svých možností a schopností minimalizovat možné dopady;
► popis způsobu řešení a zdokumentování incidentů.

Testování bezpečnosti
Účelem testování (ověřování) je zajištění úrovně zabezpečení aktiv Abc definované bezpečnostní politikou IS. Kapitola obsahuje základní schéma, podle něhož probíhá testování. Z pohledu periodicity testování jsou popsány dva základní typy testování: pravidelné testování bezpečnosti a nárazové testování bezpečnosti (vynucené okolnostmi). Kapitola také obsahuje popis kritérií, která jsou k testování použita.

7. Závěrečná ustanovení

Výjimky a sankce
V této kapitole je jasně definováno, kdo povoluje výjimky z této politiky a jaké sankce hrozí za porušení ustanovení politiky. Místo výčtu konkrétních sankcí zpravidla stačí uvedení klauzule: „Závažné porušení bezpečnostních pravidel definovaných v této politice bude považováno za porušení pracovní kázně a budou vůči pracovníkovi uplatněny odpovídající sankce."

Správa dokumentu
V této kapitole je nezbytné definovat, kdo a za jakých okolností může bezpečnostní politiku IS měnit či odvolat. Musí být popsán proces, jakým probíhá změnové řízení politiky.
V kapitole je dále užitečné uvést, jakým způsobem mohou zaměstnanci vznášet k politice připomínky.

8. Přílohy
Do této části politiky mohou být vloženy například formuláře pro připomínky k politice nebo kopie dokumentů, o nichž se v politice hovoří (certifikáty, části smluvních ujednání atd.).

9. Slovník pojmů
Ve slovníku by měly být vymezeny všechny pojmy, které mají povahu odborné terminologie nebo jejichž použití v daném kontextu může být nejasné.

Příloha č. 5: Několik ukázek phishingu

Ukázka phishingu 1 - hurikán Katrina a Červený kříž (září 2005)

Podvodníci začali registrovat doménové názvy pro stránky zaměřené na „pomoc obětem hurikánu Katrina“ a lákat peníze z dobrodinců hned, jak byl daný hurikán pojmenován a začal působit první škody.

Příklad 1: Přijde vám do schránky email se stručnými novinkami ohledně hurikánu s odkazem na další zprávy. Tato stránka se zprávami obsahuje zakódovaný javascript, který zkouší exploitovat dvě zjištěné slabiny v HTML helpu (popsané v Microsoft Security Bulletin MS05-001). Pokud počítač neobsahuje příslušné záplaty a dojde k využití alespoň jedné ze slabin, na počítač se stáhne trojský kůň. Tento kůň začne stahovat další malware, znovu trojského koně, který otevře zadní vrátka v systému a umožní útočníkovi kompletní převzetí kontroly nad počítačem.

Příklad 2: Tentokrát se jedná o podvod zaměřený na finanční dárce obětem Katriny. Doručený email je napsán v HTML a tváří se, jako by přicházel z Červeného kříže. Jako záruku „pravosti“ také obsahuje logo společnosti Verisign “Secure Site”. Po následování odkazu uvedeném v daném emailu je uživatel přesměrován na podvodnou webovou stránku hostovanou v Brazílii. Po uživateli je přes online formulář požadováno číslo kreditní karty, darovaná částka, datum vypršení platnosti a číslo PIN. Po zadání těchto údajů je uživatel přesměrován na pravé stránky Červeného kříže. [I-14]

Obrázek číslo 4: Falešná webová prezentace s darovacím formulářem

Zdroj: http://antiphishing.org (20.12.05)

Ukázka phishingu - eBay (listopad 2003)

17. listopadu 2003 dostalo mnoho zákazníků firmy eBay e-mailem upozornění, že došlo ke kompromitaci jejich účtů a tyto účty byly zablokovány. Zpráva obsahovala odkaz, který se tvářil tak, že směřuje na web eBay, kde se mohou zákazníci znovu zaregistrovat. Horní část stránky vypadala přesně jako web eBay a obsahovala interní odkazy na eBay. Pro opětovnou registraci byly od zákazníků požadovány údaje o kreditní kartě, o PINu k této kartě, o číslu sociálního pojištění, o datu narození a o rodném příjmení matky. Jediným problémem bylo, že původní e-mail neodeslala firma eBay a webová stránka také nepatřila eBay.... [I-14]

Příloha č. 6: Reakce společnosti Microsoft

V médiích a diskusních fórech jsem se velice často setkal s kritikou tohoto největšího softwarového giganta a vlastníka majoritního podílu na poli operačních systémů - společnosti Microsoft. Firmě je vyčítána ignorace současného stavu, laxnost a „děravost“ jejich aplikací. Přitom málokdo si uvědomuje složitost a délku SW kódu, nutné zajištění kompatibility a snadné propojitelnosti systémů, a v neposlední řadě fakt, že každý SW obsahuje chyby, jen u této společnosti jsou dané chyby nejvíce vidět.

Přičemž i Microsoft si plně uvědomuje vzrůstající počet bezpečnostních incidentů. V odezvě na zvyšující se útoky na své OS do nových verzí Windows XP zdarma umožňuje pro běžné uživatele přidat / automaticky přidává pomocné programy (utility) zajišťující základní prevenci proti virové nákaze či průniku špionážního software – spywaru (firewall, odstraňovač spyware a v přípravě nyní je, přes současné akvizice antivirových společností, antivir) [I-01].

Opravné balíky adresující objevené bezpečnostní chyby vydává s co možná nejmenším časovým zpožděním, rozesílá bezpečnostní zpravodaje o nových hrozbách (to, zda uživatelé tyto záplaty užívají, je již jiný problém).

Praha a Brno byly na jaře 2005 svědky konference Microsoft TechNet s názvem Den bezpečnosti počítačů, která celá byla věnována tématu odborné problematice návrhu, tvorby, nasazování a správy zabezpečené IT infrastruktury (ale již v roce 2004 se v dubnu konal v Praze Microsoft Security summit). Dále pro běžné uživatele i IT profesionály je v našich končinách nově dostupný projekt s názvem “Štít bezpečí“ [I-11], jehož cílem je poskytnout uživatelům informace o významu a důležitosti zabezpečení počítačů, ochrany dat a soukromí.

Možná ještě zajímavějším projektem, tentokrát už globálního významu, je pořádání konferencí s názvem Blue Hat. Tyto konference hodlá Microsoft pořádat dvakrát do roka; předmětem konference je setkávání zástupců firmy s počítačovými hackery, kde s nimi budou diskutovat o závažných chybách v operačních systémech Windows, které mohou umožnit napadení celých sítí. (Několik schůzek již proběhlo a Microsoft je s výsledky více než spokojen. Slovy manažera projektu Stephena Toulouse: *"Když jsou hackeři ochotni mluvit s našimi vývojáři, je to pro ně zkušenost k nezaplacení. Chceme v tom pokračovat a chceme, aby se z toho stala tradice."*). [I-03]

To, že to Microsoft se zvýšením bezpečností svých operačních systémů myslí vážně, může také ukázat velikost finanční částky, kterou společnost již v rámci iniciativy (Trustworthy Computing) vynaložila – podle hlavního bezpečnostního pracovníka Microsoft velikost této částky převyšuje náklady na neúspěšný projekt americké vlády na vytvoření protiraketového štítu s názvem Hvězdné války. [I-04]

Příloha č. 7: Plán obnovy (zálohování)

Je nutné mít data nejen zálohovaná, ale také „znovuobnovitelná“. V praxi se často stává, že podnik poctivě pravidelně provádí zálohování, ale v případě, že dojde k havárii a je potřeba data obnovit, tak se najednou zjistí, že to nejde (nenajdou se všechny zálohy, nejdou identifikovat, nejsou po ruce potřebné technické prostředky (např. softwarové vybavení).

Těmto problémům by měl předcházet plán obnovy - krizový plán, který pamatuje na souslednost jednotlivých úkonů, které je potřeba postupně vykonat, aby rekonstrukce dat byla provedena úspěšně. Plán obnovy musí být pravidelně aktualizován, aby odrážel pokud možno stále skutečný stav organizace.

V krizovém plánu je obnova dat sice podstatnou, ale nikoliv jedinou nutnou činností (je dobré znát umístění médií s poslední zálohou, znát případná hesla, kterými je záloha chráněna apod.). Nezřídka se stává, že některá data nebyla z rozličných důvodů na média zapsána, například otevřené či poškozené soubory. Je pak nutné mít podrobnou dokumentaci o provedených zálohách a vědět, co obnovit lze / nelze.

Plán obnovy by měl řešit především následující otázky: kde je možné nalézt zálohy, jakým způsobem jsou značeny, jaká technologie (HW, SW) je potřeba k jejich obnovení, jak se s ní pracuje, kdo zodpovídá za provedení obnovy dat a kdo jej zastupuje v případě nepřítomnosti, kde je možné získat přístupová hesla k chráněným zálohám apod..

Příklad časové posloupnosti akcí při obnově: oprava závady, instalace OS, rekonstrukce účtů, instalace aplikací, rekonstrukce dat, zajištění kontinuity a navazujících činností, vyvarování se provizorií i za cenu pomalejšího návratu k normálnímu stavu, obnovení zálohování.

Takto zvolený postup je nutno několikrát do roka otestovat.

Příloha č. 8: Srovnání výhod a nevýhod krátkých a dlouhých BP

Výhody krátkých BP

- relativně snadná a rychlá příprava dokumentu,
- vzhledem k rozsahu a obecnosti definovaných principů zpravidla jednodušší a rychlejší proces schvalování,
- BP není třeba příliš často aktualizovat a politika je poměrně neměnná,
- bez problémů se mohou s BP seznámit všichni zaměstnanci (dotčené osoby).

Výhody dlouhých (rozsáhlých) BP

- politika představuje velmi komplexní kodex upravující oblast informační bezpečnosti,
- definice hlavních principů a pravidel je na jednom místě,
- vzhledem k úrovni detailu je eliminována možnost případné desinterpretace nebo nepochopení,
- bezpečnostní standardy upravují velmi detailní a specifické oblasti informační bezpečnosti.

Nevýhody krátkých BP

- hlavní objem prací je přesunut do fáze rozpracování BP do formy bezpečnostních standardů,
- vzhledem k rozsahu a obecnosti definovaných principů zpravidla BP mnoho neřeší,
- pro zaměstnance (dotčené osoby) může být problém si pod obecnými principy představit jejich konkrétní náplň.

Nevýhody dlouhých (rozsáhlých) BP

- při jakékoli větší změně ve společnosti je potřeba politiku aktualizovat, tj. politika se poměrně často mění,
- práce na detailní politice mohou trvat neúměrně dlouho a existuje značné nebezpečí její nevyváženosti,
- proces schvalování politiky bývá dlouhý a komplikovaný s potřebou přijmout řadu kompromisů,
- zaměstnanci se nemohou jednoduše seznámit s celou politikou, nutno pro jednotlivé profesní (organizační) skupiny vytvořit extrakty -> další náklady.

Zdroj: [05]